



# Metasys Release 11.0 Hardening Guide



---

GPS0028-CE-20020331-EN  
Rev A

---

## Introduction



Our solution provides peace of mind to our customers with a holistic cyber mindset beginning at initial design concept, continues through product development, and is supported through deployment. Johnson Controls also includes a rapid incident response process to meet the comprehensive and evolving cybersecurity environments.

The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance specifically for the Metasys application, including Metasys software, configuration, hardware, user accounts, permissions, roles, backup, restore, and patch management. While we do provide the supported platforms, hardening of the client / server operating system, and SQL is out of scope for this document.

This Johnson Controls **Metasys Hardening guide** is broken down into three main sections depicting the overall process for hardening:

| 1. Planning   | 2. Deployment  | 3. Maintain   |
|---|--|---|
| Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening | Guides you through the execution and hardening steps based on the products and security features of the target system components | Provides a checklist for future checkpoints to keep your system safe and secure |

Appendixes are included at the end for additional Metasys literature, acronyms used within this document, and frequently asked questions (FAQs).

## **Legal disclaimer**

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

# Table of Contents

|   |    |
|---|----|
| Introduction.....   | 2  |
| Legal disclaimer.....   | 3  |
| Table of Contents .....   | 4  |
| 1 Planning.....   | 7  |
| 1.1.0 Metasys overview .....  | 7  |
| 1.1.1 Deployment architecture.....                                      | 7  |
| 1.1.2 Metasys Components.....   | 10 |
| 1.1.3 Supporting Components.....  | 11 |
| 1.1.4 Additional Deployment architecture examples .....                 | 11 |
| 1.1.5 Metasys Versions .....  | 11 |
| 1.2.0 Security feature set.....   | 12 |
| 1.2.1 Security Dashboard.....   | 13 |
| 1.2.2 Supervisory Device safeguards .....                               | 14 |
| 1.2.3 User password policy .....  | 14 |
| 1.2.4 FIPS Compliant Secure Communication on the building network ..... | 16 |
| 1.2.5 User Account Support .....  | 16 |
| 1.2.6 Encryption ciphers:.....  | 17 |
| 1.2.7 Updates.....  | 18 |
| 1.2.8 Disable insecure web traffic.....                                 | 18 |
| 1.2.9 Last Login monitoring .....                                       | 18 |
| 1.2.10 Performance Verification tool.....                               | 19 |
| 1.3.0 Intended environment .....  | 20 |
| 1.3.1 Internet connectivity .....                                       | 20 |
| 1.3.2 Integration with IT networks.....                                 | 20 |
| 1.3.3 Integration with external systems .....                           | 20 |
| 1.4.0 Patch policy .....  | 21 |
| 1.5.0 Hardening methodology.....  | 21 |
| 1.6.0 Communication.....  | 22 |
| 1.6.1 Communication port configuration .....                            | 22 |
| 1.7.0 Network planning .....  | 27 |
| 1.7.1 Trust boundaries overview .....                                   | 27 |
| 1.8.0 Hardware and software requirements .....                          | 29 |
| 2 Deployment .....  | 30 |
| 2.1.0 Deployment overview.....  | 30 |
| 2.1.1 Physical installation considerations .....                        | 30 |
| 2.1.2 Getting started.....  | 30 |
| 2.1.3 Resetting factory defaults .....                                  | 31 |
| 2.1.4 Considerations for commission.....                                | 31 |

|              |   |           |
|--------------|---|-----------|
| 2.1.5        | Recommended knowledge level .....                           | 31        |
| 2.2.0        | Hardening .....   | 32        |
| 2.2.1        | Hardening checklist .....                                   | 32        |
| 2.2.2        | Disable TLS 1.0 and 1.1 .....                               | 32        |
| 2.2.3        | Disable unused Ports .....                                  | 32        |
| 2.3.0        | User management best practices.....                         | 33        |
| 2.3.1        | Metasys User Roles and Permissions .....                    | 33        |
| 2.3.2        | Metasys Local User Accounts .....                           | 35        |
| 2.3.3        | Metasys LDAP Active Directory User Accounts:.....           | 37        |
| 2.3.4        | No shared accounts .....                                    | 37        |
| 2.3.5        | Change default passwords .....                              | 37        |
| 2.3.6        | Least privilege .....                                       | 37        |
| 2.3.7        | Separation of duties .....                                  | 37        |
| 2.3.8        | Centralized user account management .....                   | 38        |
| 2.3.9        | Password policy .....                                       | 39        |
| 2.3.10       | Kiosk Service Accounts.....                                 | 39        |
| 2.3.11       | Radius Accounts .....                                       | 39        |
| 2.3.12       | User management best practices .....                        | 39        |
| <b>2.4.0</b> | <b>Update Metasys to latest version.....</b>                | <b>40</b> |
| <b>2.5.0</b> | <b>Communication hardening.....</b>                         | <b>40</b> |
| 2.5.1        | Least functionality.....                                    | 40        |
| 2.5.2        | Communication certificate support.....                      | 41        |
| 2.5.3        | FIPS 140-2 support .....                                    | 41        |
| <b>2.6.0</b> | <b>Configuring security monitoring features.....</b>        | <b>41</b> |
| 2.6.1        | Audit Logs .....  | 41        |
| <b>2.7.0</b> | <b>Availability hardening.....</b>                          | <b>42</b> |
| 2.7.1        | Backup/restore .....  | 42        |
| <b>3</b>     | <b>Maintain.....</b>  | <b>43</b> |
| <b>3.1.0</b> | <b>Cybersecurity maintenance checklist .....</b>            | <b>43</b> |
| 3.1.1        | Backup historical data .....                                | 45        |
| 3.1.2        | Backup configuration data .....                             | 45        |
| 3.1.3        | Test backup data.....                                       | 45        |
| 3.1.4        | Disable user accounts of terminated employees.....          | 45        |
| 3.1.5        | Remove inactive user accounts.....                          | 46        |
| 3.1.6        | Update user account roles and permissions .....             | 46        |
| 3.1.7        | Disable unused features, ports, and services .....          | 46        |
| 3.1.8        | Check for and prioritize advisories or product notices..... | 47        |

|   |  |           |
|---|--|-----------|
| 3.1.9   | Plan and execute advisory recommendations .....  | 47        |
| 3.1.10  | Check and prioritize patches and updates .....   | 47        |
| 3.1.11  | Plan and execute software patches and updates.....                                     | 47        |
| 3.1.12  | Review updates to organizational policies .....  | 48        |
| 3.1.13  | Review updates to regulations.....   | 48        |
| 3.1.14  | Conduct security audits .....  | 48        |
| 3.1.15  | Update password policies.....  | 48        |
| 3.1.16  | Update as-built documentation .....  | 48        |
| 3.1.17  | Update standard operating procedures .....   | 49        |
| 3.1.18  | Update MUI logon banners.....  | 49        |
| 3.1.19  | Renew licensing agreements.....  | 49        |
| 3.1.20  | Renew support contracts.....   | 49        |
| 3.1.21  | Check for end-of-support / discontinuation information and plan for replacements. .... | 49        |
| 3.1.22  | Periodically delete sensitive data in accordance to policies or regulations.....       | 50        |
| 3.1.23  | Monitor for cyber attacks .....  | 50        |
| <b>3.2.0</b>  | <b>Metasys Release schedule .....</b>  | <b>51</b> |
| <b>Appendix A - Additional Metasys Literature .....</b> |  | <b>52</b> |
| <b>Appendix B - Acronyms .....</b>                      |  | <b>53</b> |
| <b>Appendix C – FAQs .....</b>                          |  | <b>55</b> |

# 1 Planning

This section helps plan for the implementation of security best practices for a Metasys system installation.

## 1.1.0 Metasys overview

Metasys® Building Automation System is the foundation of modern building energy management efficiency. This intelligent, world-class technology system connects your commercial HVAC, lighting, security, and protection systems – enabling them to communicate on a single platform to deliver the information you need, allowing you to make smarter, savvier decisions while enhancing your occupants' comfort, safety, and productivity.

A field engineer, or a service technician can use this document to harden a Metasys system. This document describes how to configure and use the following:

- Create unique user accounts
- Give the user sufficient permissions
- TLS/SSL and certificate management for communication between the Metasys server and the engine, or from the Metasys UI or Metasys Launcher to the Metasys device
- VPNs for remote access
- Other configurable settings

### 1.1.1 Deployment architecture

The Metasys system comprises various hardware and software components that work closely together to provide coordinated control over a site's HVAC and other building systems. More details are included in the next section - Metasys system architecture.

The Metasys system architecture is a distributed architecture. This means that the system components can be located as closely as possible to the equipment they are controlling, to provide optimum performance and reliability. The distributed Metasys components with their data sources and the equipment they control are connected by:

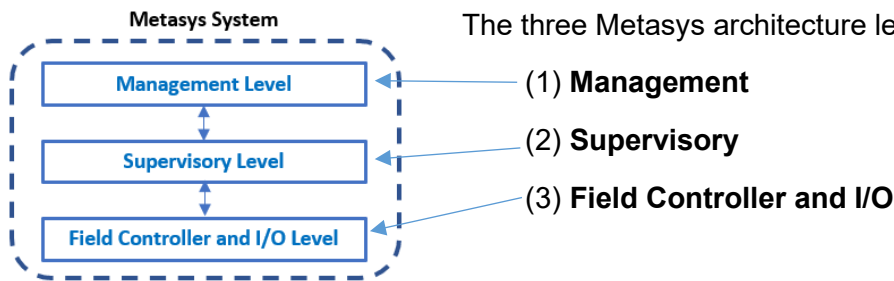
- Direct wiring
- Network wiring
- Wireless networking

The distributed Metasys components and various connection methods ensure system-wide data sharing, coordination, and remote access.

The Metasys system architecture is scalable. This means that you can add components as required to:

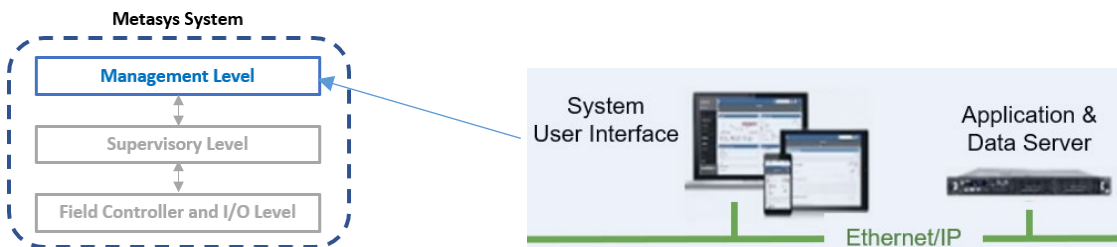
- Control buildings and systems of varying complexity, size, and scope
- Integrate third-party devices to unify their operation with the Metasys system
- Integrate earlier generations of Metasys components to modernize and unify their operation

It is important to note that every installation is unique. However, each installation can be broken down into basic building blocks or "Levels" which make up every Metasys installation.

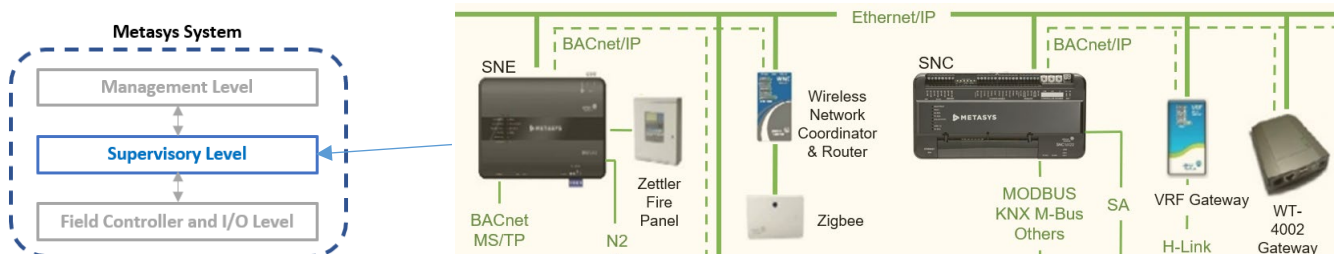


The management level resides on an Ethernet network which connects the engines. Within the supervisory level, engines route to the field controller network which can be IP-based as well as serial-based networks, while I/O devices often connect to field controllers using a standard electrical interface (e.g., voltage, current, pulse, or contact). However, some I/O devices are communication using a protocol interface.

**Management Level.** The Management level includes the system user interface and the server (or multiple servers) that hosts the application and database. These are core components and will be discussed further in the deployment architecture section.



**Supervisory Level.** The Supervisory or Engine level coordinate communications between the Management level and the Field controller and I/O level



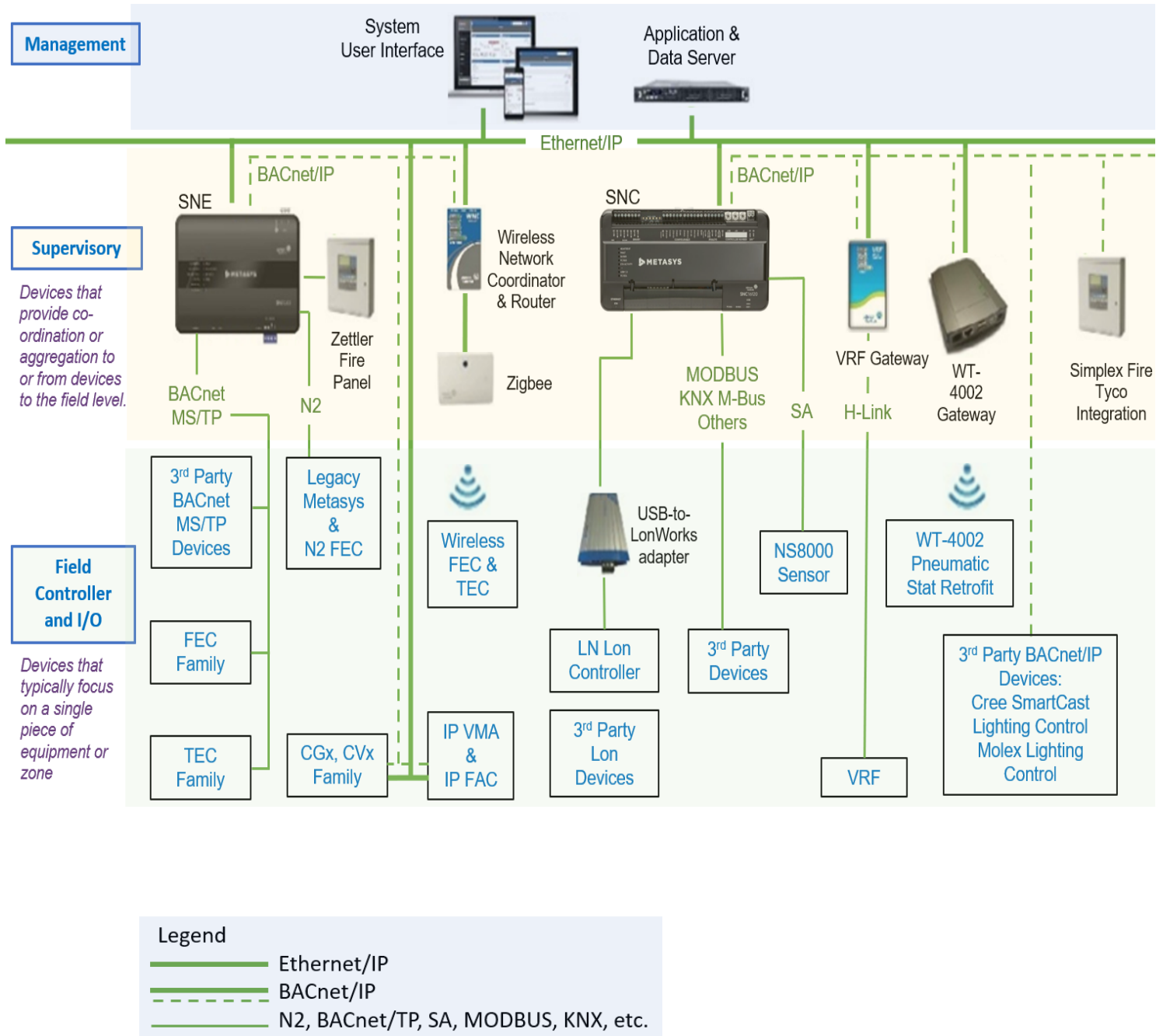
**Field Controller and I/O Level.** The Field Controller and I/O level includes the equipment controllers and communicates back to the Supervisory Level





Section 1.1.2 Metasys Components describes the components that make up each level in further detail

Figure 1.1.2: Metasys system architecture example



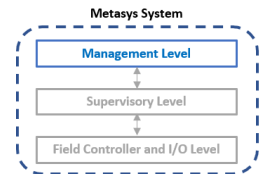
## 1.1.2 Metasys Components

The Metasys System configuration includes one to many Server, Network and Field components, which work together to provide a custom solution. The sections below contain a subset of the many components that may be included in a custom solution. For more comprehensive listing of devices and documentation of components Metasys supports, refer to **Appendix A - Additional Literature**.

### 1.1.2.1 Management Level – A site can optionally have one or more Metasys servers—computer-based devices that add long-term data storage and support for larger Metasys networks.

Metasys server products include:

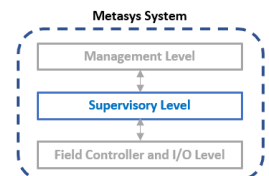
- a. Application and Data Server (ADS)
- b. ADS-Lite (available only in specific markets)
- c. Extended Application and Data Server (ADX)
- d. Open Application Server (OAS)



### 1.1.2.2 Supervisory Level – Network Engines provide network management and system-wide control coordination over one or more networks of equipment controllers.

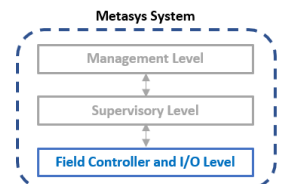
Network components include:

- a. Network Automation Engine (NAE)
- b. Network Control Engine (NCE)
- c. Network Integration Engine (NIE)
- d. Series Network Engine (SNE)
- e. Series Network Control Engine (SNC)
- f. Device gateway
- g. Server based engines such as NAE8500 or LCS8520



### 1.1.2.3 Field Controller and I/O Level – Metasys includes several model series of equipment controllers, including Various equipment controllers

- a. Application Controller (CGM/CGE)
- b. VAV Box Controller (CVM – field RJ45)
- c. Advanced Application Field Equipment, Controller (FAC)
- d. Field Equipment Controller (FEC)
- e. Variable Air Volume Modular Assembly (VMA)
- f. Terminal Equipment Controller (TEC)
- g. Legacy Metasys controller, such as Unitary (UNT) controller, Variable Air Volume Assembly and Air Handler Unit (AHU) - List from Carol
- h. Input/Output Modules (IOMs)
- i. Expansion Modules (XPM)
- j. Sensor Actuator (SA) bus devices
  - a. Network sensors (NS8000s)
  - b. Actuators
  - c. Generic SA bus device
  - d. VFD on the SA bus



### 1.1.3 Supporting Components

Metasys is designed to be compatible with standard protocols. With built-in support for BACnet, Lon, Modbus, and other Johnson Controls systems, it is possible to interoperate with devices which support those protocols that were not specifically developed for Metasys. Networking components are also often included as part of the deployment architecture. Some components such as a Router and/or Smart Switch may be pre-existing, on site, supplied by the customer.

NOTE: Details on hardening Supporting Components are out of scope not included within this guide.

#### Management Level

- a. Third party management system which Metasys integrates to (BACnet, OPC UA)

#### Supervisory Level

- b. BACnet Building Controller (B-BC) - Controllers conforming with BACnet Building Controller device profile

#### Field Controller and I/O Level

- a. N2 Field Controller - The N2 Field Equipment Controller legacy family comprises a group of versatile controllers and accessories designed to monitor and operate a wide variety of commercial HVAC equipment and can be networked together using the N2 Open Communications protocol (Serial network).
- b. BACnet Field Controller – BACnet IP or BACnet MS/TP serial controllers
- c. Lon Field Controller – Controllers that utilize the standard LonTalk protocol
- d. Other protocol controller
- e. Input/Output (I/O) Devices – IP or Serial I/O devices which communicate to other system components using a protocol (BACnet, LON, N2, Modbus, etc.)

#### Networking

- a. Router (i.e., Edge router, Loytec BACnet/IP, remote field bus, etc.)
- b. Smart Switch (i.e., Smart ethernet switch, Netgear, Cisco, CCSI, etc.)
  - a. Ring Manager – IE2000 and IE4000 with Media Redundancy Protocol (MRP) for IP controllers

### 1.1.4 Additional Deployment architecture examples

Figure 1.2, above in section 1.1.1, showed one example deployment with various components.

See the Metasys System Configuration Guide for Metasys Release 11.0 (LIT-12011832) for additional details and configuration options.

### 1.1.5 Metasys Versions

Johnson Controls advises Metasys customers to upgrade to the latest release which would ensure you have the latest features and most secure installation. If you have a system that requires the ADX as a server, it must be at the highest release number. Its child engines can be at 11.0 or mixed with a lower version (not below 5.2). Because you should take advantage of cybersecurity features, it is recommended that all engines are at 10.1 and higher.

**Note:** Some engines cannot go above 9.x and should be part of an upgrade plan. See Metasys Server Installation and Upgrade Instructions (LIT-12012162) for additional details.

Specific Series Network Engine models for Metasys Release 11 (newest release at the time this guide was written) are:

| Supported Hardware | SNE2200x     | SNE1100x     | SNE1050x     | SNE110Lx   |
|--------------------|--------------|--------------|--------------|------------|
| Succeeds           | NAE55 series | NAE45 series | NAE35 series | NAE45-Lite |

Specific Series Network Controller models for Metasys Release 11 (newest release at the time this guide was written) are:

| Supported Hardware | SNC2515x-0<br>SNC2515x-0H | SNC2515x-04<br>SNC2515x-04H | SNC1612x-0<br>SNC1612x-0H | SNC1612x-04<br>SNC1612x-04H |
|--------------------|---------------------------|-----------------------------|---------------------------|-----------------------------|
| Succeeds           | NCE25 Series              | NCE25 Series                | NCE25 Series              | NCE25 Series                |

See Metasys System Product Bulletin (LIT-1201526) for additional details.

### 1.2.0 Security feature set

The Metasys UI supports the security features shown in the table below.

The column titled “Feature Available” shows the first release when this feature became available. For example, if you are running Metasys version 9.0 and a certain feature you are looking to deploy started with version 10.0, then you would need to update to version 10.0 or higher to use this feature.

Table 1.2.0

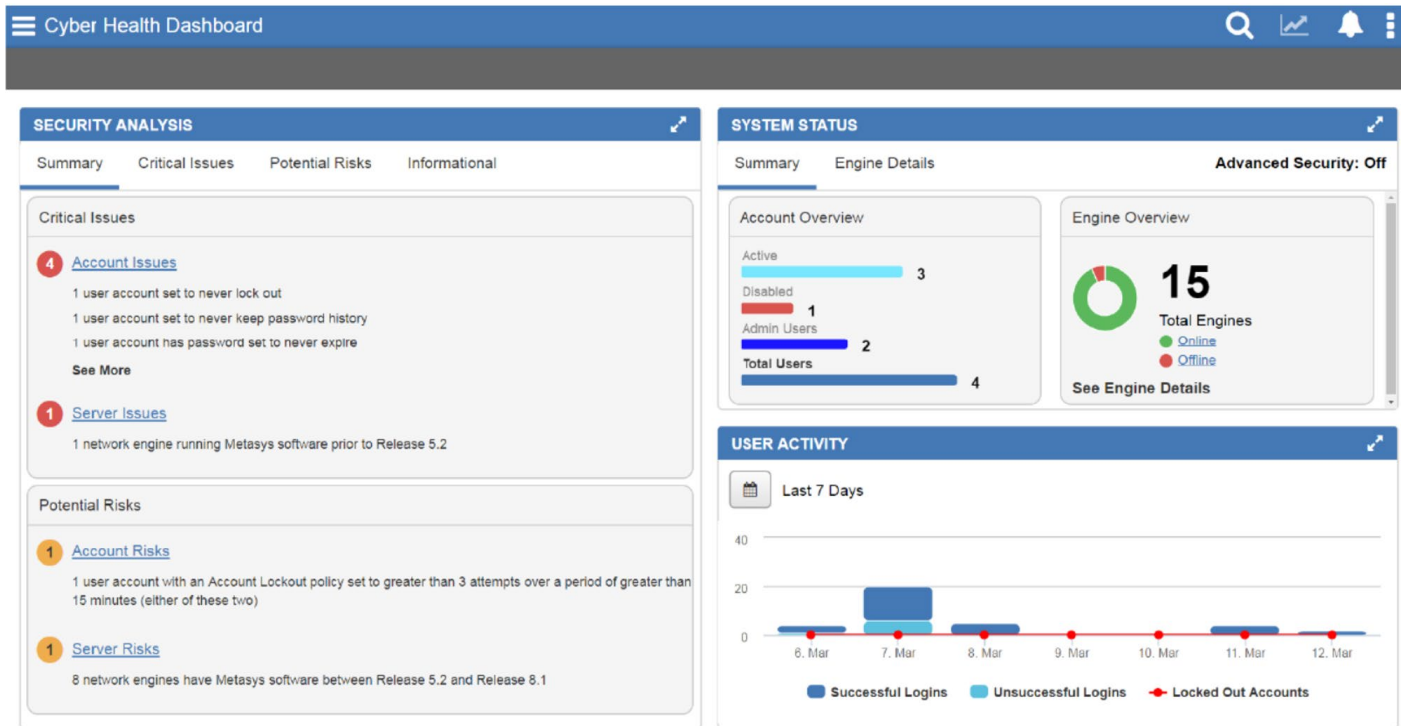
| Section | Type  | Feature name                             | Feature Available |
|---------|---|--|-------------------|
| 1.2.1   | Cybersecurity Dashboard (Metasys User Interface MUI only) | Security Analysis widget                 | 10.1              |
|         |   | System Status                            | 10.1              |
|         |   | User Activity widget                     | 10.1              |
| 1.2.2   | Supervisory Device safeguards                             | Advanced Security Enabled                | 10.0              |
|         |   | Engine Pairing                           | 10.0              |
| 1.2.3   | User password policy                                      | User account control                     |                   |
| 1.2.4   | Secure Communication on the building network              | FIPS 140-2 Compliance                    | 11.0              |
| 1.2.5   | User Account Support                                      | Identify Dormant or unused user accounts | 8.0               |
|         |   | User account management                  | 7.0               |
|         |   | Warning Banner for unauthorized users    | 8.0               |
|         |   | Inactive Sessions                        | 7.0               |
| 1.2.6   | Encryption ciphers  | Cipher support                           |                   |
| 1.2.7   | Updates   | Update messages                          |                   |
| 1.2.8   | Disable insecure web traffic                              | Allow HTTPS                              | 8.1               |
| 1.2.9   | Monitor   | Audit Log                                | 1.0               |
|         |   | Last Login                               | 8.0               |
|         |   | DDA using Syslog                         | 7.0               |

**Note:** Some of these features require configuration and/or licensing to be activated. See section 2 for additional details.

### 1.2.1 Security Dashboard

The Cyber Health dashboard provides a Metasys Administrator with a centralized view of potential security related issues or system issues which are detectable by an OAS and ADy, which may not surface as part of general system alarms. The administrator can also view if any software needs to be updated.

Figure 1.2.1 Cyber Health Dashboard



**Security Analysis widget.** This feature Provides a detailed breakdown of the Critical Issues and Potential Risks present with accounts and servers, along with an Informational tab showing the number of total users accounts and more. The Metasys UI makes it easy to view items such as:

- The status of all user accounts (active, dormant, locked, temporary, disabled, administrator)
- Out-of-date software
- Certificate expiration, version, and status of engines

**System Status Widget.** Shows an account overview in the form of a bar chart and an engine overview in the form of a doughnut chart. The Engine Details tab lists the name, IP address, certification expiration, firmware version, and status of the engines.

**User Activity Widget.** The User activity widget shows in a dashboard view important events, such as:

- Successful user login occurrences during a specified period.
- Unsuccessful user login occurrences during a specified period.
- Account lock-out occurrences during a specified period

## 1.2.2 Supervisory Device safeguards

The Advanced Security Enabled and Engine Pairing provide an improved level of security between Metasys Site Directors and devices

**Advanced Security Enabled.** When enabled on a Site Director at Metasys 10.0 or later, the Advanced Security Enabled attribute rejects all communication attempts from network engines that have not been paired. The setting applies to the entire site, and only works with engines at Release 10.0 or later. When this attribute is set to True, a user message appears to indicate that all network engines prior to Release 10.0 remain functional but are disconnected from the site because they are no longer allowed to communicate with the Site Director.

**Engine Pairing.** Beginning at Metasys Release 10.0, a more secure authentication process has been implemented between updated engines and the Site Director that involves device pairing. After you pair an NxE with a Site Director, the two devices use unique credentials to authenticate communication between them. Engines at 10.x and greater must be paired to communicate with a Site Director. Unpaired engines are not able to communicate with a Site Director.

**Encrypted Communication.** Once devices are installed with or upgraded to Release 8.1 or later, Metasys system communication between ADX/ADS/NxE/SNx/OAS/SMP UI/Metasys UI is encrypted. Child devices at Release 8.0 or prior can be used on a Release 8.1 or later site, but communications will remain partially unencrypted. Optionally, the customer's IT department can generate trusted certificates for the Metasys Site Director. These certificates provide encrypted and trusted communication between the Site Director and the client. Trusted certificates from a Certificate Authority (CA) can be used on a new Metasys system, to provide encrypted and trusted communication between the Site Director and the Metasys SMP.

## 1.2.3 User password policy

Using Metasys user interface (MUI) and the Site Management Portal (SMP) UI you can apply a role-based account.

**User account control.** User accounts control user access to the Metasys system. An account defines which portions of the Metasys data a user can access (for example, all HVAC data or all lighting data from a particular area of the building) and which functions the user can perform on that data, from view-only access to configuring new databases. Always use the Principle of Least Privilege which states each user account should be given only those privileges needed to complete their tasks. The Metasys system provides the ability to divide the data into 163 unique categories, including HVAC, Fire, and Security; and has 10 different levels of user functionality.

Users can further limit user accounts to operate only at specified times on specified days of the week. The System Administrator creates all account settings.

Each account can also have associated preferences, such as which graphic or trend to display when a user logs in to the SMP UI, or which User Views appear in the Navigation Tree.

Basic Access is a feature through which users can create limited operator access to SMP features based on the user's assigned permissions in the Security Administrator. Users can avail of Basic Access on all the Metasys system engines and servers.

## Microsoft Active Directory

The SMP and Metasys UI can use Microsoft Active Directory® LDAP accounts.

Table 1.2.3 shows the products which support Active Directory (AD) logins and Single Sign On (SSO).

Table 1.2.3 Metasys products AD &amp; SSO logins

| Application                                    | AD login support | Exact or alternate UPN format login support | SSO Support |
|--|------------------|---|-------------|
| <b>ADS/ADX Site Management portal UI</b>       | Yes              | Yes   | Yes         |
| <b>SCT*</b>                                    | Yes              | Yes   | Yes         |
| <b>SCT Pro</b>                                 | Yes              | Yes   | No          |
| <b>Metasys UI and Metasys UI Offline</b>       | Yes              | Yes   | No          |
| <b>OAS</b>                                     | Yes              | Yes   | Yes         |
| <b>Metasys Advanced Reporting System</b>       | No               | No  | No          |
| <b>Network Engine (H/W and Server version)</b> | No               | No  | No          |
| <b>Metasys for Validated Environments</b>      | Yes              | Yes   | No          |

\* SCT 15 has AD LDAP capability and AD SSO (but no ADFS integration)

See section 2.3 for additional details about user account management guidelines.

### Active Directory Federation Service (ADFS) two-factor authentication

Two-factor or multi-factor authentication (MFA) is a method to login after the user has presented two or more pieces of evidence. In addition to their username, a user will provide an additional identification verification such as scanning a fingerprint, or a code received from a mobile device.

Integration with two-factor authentication is an ADFS add-on, licensed feature to add support for Metasys using ADFS, a single sign-on solution developed by Microsoft®. ADFS can then, in turn, be used to provide two-factor authentication for access to Metasys. ADFS, a centralized user account management feature, helps prevent unauthorized access to Metasys, which if not prevented, could result in data, financial, and reputational loss, system disruption, and other negative consequences.

#### Notes:

- ADFS is available in Metasys UI for the ADX, mobile phones and tablets.
- ADFS is not available to Metasys SMP users.
- The ADFS single sign-on and two-factor authentication are configured on the customer's ADFS system.
- Please refer to the Metasys System Configuration Guide Release 11.0 (LIT-12011832) for additional details.
- Metasys supports ADFS 4.0 and higher

| Application | AD login support | SSO Support |
|-------------|------------------|-------------|
| <b>MUI</b>  | X                | X           |
|             |                  |             |

## 1.2.4 FIPS Compliant Secure Communication on the building network

### 1.2.4.1 FIPS 140-2 Standard and Definition

The Federal Information Processing Standard (FIPS) publication 140-2 is a U.S. government standard that specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

NOTE: on a FIPS enabled site, engines earlier than release 11.0 will not be able to communicate with the site director.

See this NIST link for more details - FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov).

### 1.2.4.1 FIPS 140-2 and Metasys

FIPS 140-2 is a licensed add-on feature to the Metasys Server software products, including ADS, ADX, NAE8500, and OAS and provides FIPS 140-2 compliance. When FIPS 140-2 is used, any engines on the site must also be upgraded to Release 11.0 or later.

FIPS 140-2 compliance is automatically available on engine-based sites at Release 11.0 and requires that all child-engines are also upgraded to Release 11.0 FIPS 140-2 certification can be obtained by using the SNx at Metasys Release 11.0 or later for the site director and child engines.

For the server class products ADX/ADS/OAS/NAE8500, one must purchase the FIPS-140-0 product code and license it. The specific product code is M4-FIPS-0.

Here is a list of the Metasys devices that support FIPS 140-2:

| Metasys Device | Device Type | FIPS Compliant | FIPS Certified |
|----------------|-------------|----------------|----------------|
| ADX / ADS      | Server      | Yes            |                |
| OAS            | Server      | Yes            |                |
| NAE8500        | Engine      | Yes            |                |
| NAE55          | Engine      | Yes            |                |
| SNE/SNC        | Engine      | Yes            | Yes            |

For information on wolfCrypt FIPS Certificate #3389 (NIST) visit this [Link](#).

## 1.2.5 User Account Support

**Dormant accounts.** The Potential Risks tab on the Cyber Health dashboard in Metasys UI provides a Metasys administrator with a centralized view of account users, including Dormant User Accounts.

The Dormant Account User Report in SMP is used to identify and deactivate accounts designated as inactive or disabled. The report shows Active Directory, and local dormant accounts for supervisory devices (NxE, ADX/ODS/OAS) at Metasys 8.0 or later. See Metasys 11.0 Security Administrator System Technical Bulletin (LIT-1201528 Tables 20 and 21) for details how to ensure this feature is enabled.

An optional alarm can be set to identify dormant accounts on an ADS/ADX/ODS/OAS. While the alarm does not include engines, this information can be gathered by running a report on demand. When a dormant account is detected, you may choose to lock out the account, receive an alarm or both.

**User account policies.** Administrators manage the settings of each individual user account to match their preferred settings. Adjustments can be done for inactive sessions, account lockout, dormant accounts, and password policies. Each feature provides protection from unauthorized users.



**Password History.** Keeps history and ensures password cannot be reused

**Password Aging.** Configurable time before a user is required to change their password

**Warning Banners.** Warning banners are a special login feature that consists of a text window that appears to the user during login. The banner provides a definitive warning towards any possible intruders that may want to access your system that certain types of activity are illegal. At the same time, it also advises authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s). The information in the text window may be customized for a United States government agency where the Metasys system is installed. Three different warning banners are available:

- U.S. Department of Defense (DoD)
- U.S. General Services Administration (GSA)
- U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA).

During the login process, and with one Warning Logon Banner active, Metasys can capture the client IP address of the machine a user logs in with. For higher security, user logins can be recorded from a camera to link the image of the person logging on with the user credentials to aid forensics for any suspected illegal activities. This higher security and camera would be provided outside of Metasys.

**Inactive Sessions.** Timed logout automatically logs you out of the Metasys system after a predefined time of inactivity. The system closes open databases, discards unsaved changes and view settings, and logs out the user. The session time out is noted in the Metasys audit log.

#### 1.2.6 Encryption ciphers:

For Metasys Hardware engines these ciphers have been valid since release 9.0.7. There are more cipher suites available with PC and Server Operating systems, but they are subject to negotiations when a HTTPS session is initiated. In that case, the hardware NAE/SNx would drive the cipher suites towards the ones that they support.

```

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256

```

For Metasys ADX servers we use ciphers that are provided by Microsoft SChannel for each operating system listed in the System Configuration Tool Catalog Page (LIT-1900198). The Metasys application does not encourage the use of TLS 1.0 or TLS 1.1.

## 1.2.7 Updates

### Updates tab overview

The Updates tab displays information about the available updates for installed Johnson Controls software. You can download the files you need to complete the update from the Updates tab. To open the tab, click on the Updates tab.

Click the Refresh icon on the Updates tab to complete a manual refresh and get new updates if available. From the time you click the refresh icon on the Updates tab until the refresh is in progress and the system is establishing a connection with the server, you cannot change the connection setting, change the proxy details, download, resume a download, or cancel a download. Note: When you turn on the machine, the Software Manager checks when the scheduled refresh last occurred on that machine. If the scheduled refresh has not occurred in the past 12 hours and is not set up within 30 minutes when the user turns on the machine, the system runs the scheduler automatically to get the latest updates.

The following messages may display in the Updates tab based on different scenarios:

- No updates are available in the system: No new available updates. The latest version is installed.
- Online connection setting is set to None (Offline): Software Updates are not available when the online connection setting is None (Offline).
- Installed version of the product is EOL and no updates are available: This product has been discontinued. Please contact your sales representative for further details.
- Installed version of the product is EOL but some updates are available: The installed product has been discontinued. Please download and install the latest version.

For additional information see the following:

- Software Manager Help (LIT-12012389) for additional information
- Section 3.1.12 Plan and execute software patches and updates
- Section 1.3.1 Internet connectivity, which is required for Software Manager. There is a manual procedure if you cannot open a port at the site.

Metasys uses secure HTTP with Transport Layer Security (TLS) 1.2 between the SCT computer, all Metasys servers, and network engines that are upgraded to Metasys Release 8.1 and later. The encrypted HTTPS communications apply to the Metasys servers, Metasys UI, network engines, and SCT. This ensures that unauthorized users and computer hackers cannot view the contents of communications sent between Metasys equipment and user interface clients.

## 1.2.8 Disable insecure web traffic

Metasys uses secure HTTP with Transport Layer Security (TLS) 1.2 between the SCT computer, all Metasys servers, and network engines that are upgraded to Metasys Release 8.1 and later. The encrypted HTTPS communications apply to the Metasys servers, Metasys UI, network engines, and SCT. This ensures that unauthorized users and computer hackers cannot view the contents of communications sent between Metasys equipment and user interface clients.

## 1.2.9 Last Login monitoring

The main screen of the Metasys server or SCT user interface indicates the last time and date that user successfully logged in. The Metasys username displayed on the Site Management Portal (SMP) and MUI user interface is partially obscured after a successful login. For enhanced security, only the first three characters of the username are displayed, followed by three asterisks. If the user has never logged in, "Never" appears in the Last Login field. See figures 1.2.9.1 and 1.2.9.2.

Figure 1.2.9.1

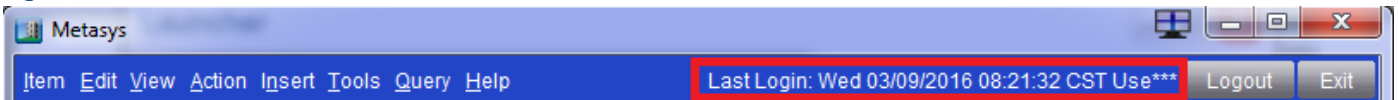





Figure 1.2.9.2



When a user logs on to either Metasys interface, the color of the lock will indicate Level and trust.

| Indicator  | Description                          | Status   |
|--|--------------------------------------|--|
|   | Green shield with check mark         | Security level between the client computer and the Metasys Server or network engine is encrypted and trusted.  |
|   | Orange shield with exclamation point | Security level between the client computer and the Metasys Server or network engine is encrypted, but not trusted.   |
|  | Red shield with X symbol             | Security level between the client computer and the Metasys Server or network engine cannot be verified because the certificate has expired, is not valid, or is not present. However, if the client computer is using Launcher 1.6 and the Metasys Server or network engine is at Release 8.1, communication is still encrypted. |

### 1.2.10 Performance Verification tool

The Metasys Performance Verification Tool (PVT) is a tool that was developed by Johnson Controls to help document hardware inventory, identify outdated items, assist with upgrades, and help with cybersecurity.

The following tasks can be easily performed using the PVT:

- Overall
  - Determine the overall health of the Metasys system
  - Identifies whether all points are categorized the same
- Equipment
  - Scan one server at a time to identify an inventory list of all the controls hardware
  - Identify the equipment the system controls
- User accounts
  - Identifies whether the MetasysSysAgent Default user and password are being used
  - List user accounts who possess administrator privileges
  - Identifies user accounts that have not logged into Metasys within the last six months

For additional information see Metasys Performance Verification Tool (PVT) User Guide (LIT-12012406).

Note: PVT is only compatible with Metasys Release 7.0 or later.

### 1.3.0 Intended environment

Physical access and installation of Metasys devices can greatly impact cybersecurity. Many Metasys components are designed to be operated in an indoor, dry environment. However, components at each level will possess varying degrees of access.

Management Level – The Metasys server is to be installed on location within an equipment rack in a secured, temperature-controlled location, such as within a data center or IT Server room with restricted access.

Supervisory Level – These components are designed to be installed in a user supplied panel or enclosure in an upright orientation. In most cases devices should also be physically secure, i.e., mechanical, and electrical rooms. The panel or enclosure should also be locked. Install in areas free of corrosive vapors and where the ambient temperature stays below 122 degrees F (50 degrees C).

I/O Field controller Level – This level has a vast listing of components that may be included in your system. Because of this, we can offer broad environmental information. For example:

- Components may be mounted horizontally or vertically
- It is recommended that the installation location is dry, away from corrosive vapors, away from electromagnetic emissions
- If possible, do not mount on surfaces prone to vibration
- Provide sufficient space for cover removal, cabling and wired connections

For more information, review the specific installation instructions of your Metasys components.

#### 1.3.1 Internet connectivity

Connecting any Operational Technology (OT) System to the internet always increases cybersecurity risk. To harden your system, Johnson Controls recommends that you do not connect Metasys directly to the internet. For Metasys this could mean

- Opening the web server to the internet
- Allowing inbound access to the ADX (high-risk)

#### 1.3.2 Integration with IT networks

Engage appropriate network security professionals to ensure that the computer hosting the Site Director is a secure host for Internet access. Network security is an important issue. Typically for existing building installations, the IT organization must approve configurations that expose networks to the Internet. For new building installations follow the JCI recommendations. Be sure to fully read and understand IT Compliance documentation for your site.

#### 1.3.3 Integration with external systems

Microsoft Active Directory LDAP or ADFS services

This section provides an overview of Active Directory LDAP services as implemented in the Metasys system. For more details, refer to the Security Administrator System Technical Bulletin Release 11.0 (LIT-1201528).

The Active Directory service feature used by the Metasys system provides an IT standard integration of the Metasys system into a customer's existing Active Directory service infrastructure for authentication purposes. This optional component provides the convenience of Single Sign-On (SSO) access for some Metasys products, a capability that permits users to log in to multiple, secured application User Interfaces without re-entering their username and password.

The Metasys system works in conjunction with the Active Directory Service. It allows the Active Directory Service to provide authentication for access to various Metasys software applications, including the Metasys ADX / ADS / OAS server, Metasys UI, Metasys UI Offline, and System Configuration Tool (SCT) (but not the engines). Using the Security Administrator System menu option, you can add Active Directory users and assign them various levels of access and permissions, from read-only to administrator privileges. By using the Security Administrator System option, you can also grant SSO or Single Sign-On access to all Active Directory users for a more convenient authentication process. The Metasys UI and Metasys UI Offline does not support SSO.

The Metasys architecture uses Active Directory service for authentication. The user provides Active Directory service credentials in one of two forms:

- Active Directory service credentials that are cached by Windows when the user logs in to the computer, and then automatically retrieved by the Metasys system during the Windows Integrated Authentication with IIS process on the Metasys server, or SCT.
- Active Directory service credentials (username, password, and domain) that are specified directly on the Site Management Portal UI login screen.

An Active Directory service username includes the specification of a domain name with the username. For example, instead of a username called John, the username in Active Directory service and the Metasys system could be John@my.corp.com, which includes the domain specifier required by Active Directory service.

Optionally, Metasys can be configured to send audits / Event alarms to up to three external Syslog servers.

#### **1.4.0 Patch policy**

The policy documented here sets forth the current internal operating guidelines and process regarding Metasys, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavours to address issues that arise within Metasys with the severity that they warrant.

When CRITICAL security vulnerabilities are discovered within Metasys, Johnson Controls will use commercially reasonable efforts to issue a critical patch for the current version of Metasys.

When non-CRITICAL vulnerabilities are discovered within Metasys, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release of Metasys
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases of Metasys

#### **1.5.0 Hardening methodology**

While Metasys provides many onboard security safeguards, including secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, Deployment.

Generally, a defense-in-depth strategy employing standard IT hardening methods and compensating controls is needed to compliment the base security features of each component.

## 1.6.0 Communication

### 1.6.1 Communication port configuration

In a Metasys system, when you use a feature that requires a communication protocol, ensure that the corresponding port is open. Hardening your system involves closing any port that is not used. The tables on the following pages provide information on ports and protocols for Metasys to function properly.

Over the next several pages, you'll find the following three tables that relate to Metasys ports.

- Table 1.6.1.1 - Internal and External TCP/IP Port numbers and protocols
- Table 1.6.1.2 - Internal Only Port numbers and protocols
- Table 1.6.1.3 - Wireless Port numbers and protocols

Table 1.6.1.1: Internal and External TCP/IP Port numbers and protocols

| Port      | Protocol | Use        | Devices   | Inbound/<br>Outbound | Description  |
|-----------|----------|------------|---|----------------------|--|
| 22        | SSH      | TCP        | Network Engine<br>(Linux only)  |                      | Used to remotely access a network engine from a laptop. This function is only available for use by authorized personnel on Johnson Controls laptops.   |
| 23        | Telnet   | TCP        | Network Engine  |                      | Telnet is no longer available for network engines at Release 10.0 or later.  |
| 25        | SMTP     | TCP        | ADS/ADX/OAS/ODS<br>Network Engine                                     | O                    | Used for alarms and events.  |
| 53        | DNS      | UDP        | Active Directory<br>Client  | I/O                  | Translates domain names into numerical IP addresses. This port allows the server to receive responses to DNS queries.  |
|           |          |            | ADS/ADX/OAS/ODS<br>Computer (Web<br>Browser)                          | I/O                  |  |
|           |          |            | Network Engine  | I/O                  |  |
| 67,<br>68 | DHCP     | UDP        | Active Directory<br>Client  | I/O                  | Assigns and keeps track of dynamic IP addresses and other network configuration parameters.<br><b>Alternate Method:</b> Use static IP addresses.   |
|           |          |            | ADS/ADX/OAS/ODS<br>Computer (Web<br>Browser)                          | I/O                  |  |
|           |          |            | Network Engine  | I/O                  |  |
| 69        | TFTP     | UDP        | Network Engine  | I/O                  | Downloads new images to NAEs<br><b>Note:</b> This port is used only when the NAE is provisioned (Not used during system runtime).  |
| 80        | HTTP     | TCP        | ADS/ADX/OAS/ODS<br>Computer (Web<br>Browser)<br>Network Engine<br>SCT | I                    | Provides communication between peer controllers, computers, and other Internet systems using SOAP over HTTP. The ADS/ ADX/ODS requires that only Port 80 be open to receive communication from client devices. Port 80 is the primary port used by the World Wide Web.<br>Note: For a higher level of security, at Metasys system Release 8.1 or later, you can close Port 80 (incoming and outgoing). |
| 80        | HTTP     | TCP        | NAE Update Tool   | I                    | Used for file transfer between the client computer and the network engine.   |
| 88        | Kerberos | TCP<br>UDP | ADS/ADX/OAS/ODS<br>(Domain X member)                                  | I/O                  | Used by the Metasys system for Active Directory service authentication at the  |

|     |                             |     |  |                          |   |
|-----|-----------------------------|-----|--|--------------------------|---|
|     |                             |     | ADX Split Web/Application Server (Domain X member)<br>Metasys System Client (Any Domain member)<br>SCT (Domain X member)                                   | I/O<br>I/O<br>I/O        | Metasys system login screen, and Service Account authentication prior to LDAP queries. Kerberos is a standard network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos is the primary security protocol for authentication within an Active Directory service Domain. Kerberos authentication relies on client functionality built into the Windows operating systems supported by Metasys software. |
| 110 | POP3                        | TCP | Computer (Web Browser)   | O                        | Receives and holds email for downloading from your Internet server. POP3 is allowed in the Metasys system only for authentication from a SMTP server.<br>Note: Firewall rules are usually unnecessary to allow access because this server should be behind the firewall.  |
| 123 | NTP                         | UDP | ADS/ADX/OAS/ODS (Domain X member)<br>ADX Split Web/Application Server (Domain X member)<br>Metasys System Client (Any Domain member) SCT (Domain X member) | I/O<br>I/O<br>I/O<br>I/O | Used for time synchronization across a network between client computers and server class operating system host computers.   |
| 123 | SNTP                        | UDP | ADS/ADX/OAS/ODS Network Engine   | I/O<br>I/O               | Used to synchronize computer clocks over a network between a server and its clients. SNTP is not required for all systems.  |
| 135 | Remote Procedure Call (RPC) | TCP | ADS/ADX/OAS/ODS (Domain X member)<br>ADX Split Web/Application Server (Domain X member)<br>Metasys System Client (Any Domain member) SCT (Domain X member) | I/O<br>I/O<br>I/O<br>I/O | Used by IIS on the ADS/ADX, OAS/ODS, and SCT during the process of authentication during SSO (Windows Integrated Authentication). If SSO is disabled in the Metasys system, this port and protocol are not used by the Metasys system; however, if the ADS/ADX, OAS/ODS, SCT, or Metasys client, or any combination are members of an Active Directory service domain, this port and protocol are used for Active Directory service functionality.  |
| 161 | SNMP                        | UDP | ADS/ADX/OAS/ODS<br>Metasys UI<br>Network Engine<br>SCT   | O<br>O<br>O<br>O         | Provides network monitoring and maintenance. Typically notifies IT department personnel of alarms that are of interest to them, such as data center environmental conditions. The site must use a network management system capable of receiving SNMP Traps.  |
| 162 | SNMP Trap                   | UDP | SCT Pro/NCT Tool   | I                        | Used by Metasys devices at start up, this port announces discovery-related information.   |
| 389 | LDAP                        | TCP | ADS/ADX/OAS/ODS (Domain X member)  | I/O                      | Used by the Metasys system to access user objects and attributes within Active  |

|      |                                   |     |   |     |   |
|------|-----------------------------------|-----|---|-----|---|
|      |                                   |     | ADX Split Web/Application Server (Domain X member)              | I/O | Directory service.  |
|      |                                   |     | Metasys System Client (Any Domain member) SCT (Domain X member) | I/O |   |
| 443  | SSL                               | TCP | ADS/ADX/OAS/ ODS (Domain X member)                              | I/O | Required if you use SSL with your reporting ADX.  |
|      |                                   |     | Metasys Advanced Reporting ADX                                  | I   |   |
| 443  | TLS                               | TCP | NE55/SNx/NAE85 Network Engine SCT (Domain X member)             | I/O | Required if you use TLS with the Metasys UI and the Metasys UI Offline for site security. Port 443 is used for secure web browser communication. Data transferred across such connections is highly resistant to eavesdropping and interception. Moreover, the identity of the remotely connected server can be verified with significant confidence. Web servers offering to accept and establish secure connections listen on this port for connections from web browsers desiring strong communication security. |
|      |                                   |     | Metasys UI and Metasys UI Offline Computer (Web Browser)        | I   |   |
|      |                                   |     |   | O   |   |
| 443  | HTTPS                             | TCP | Background File Transfer (BFT) in SCT                           | I   | With BFT, file transfers occur between the device and SCT where the device is the HTTPS client and SCT is the HTTPS server.   |
| 445  | NT LAN Manager Version 2 (NTLMv2) | TCP | ADS/ADX/OAS/ODS (Domain X member)                               | I/O | Used during Metasys system SSO authentication.  |
|      |                                   |     | ADX Split Web/Application Server (Domain X member)              | I/O |   |
|      |                                   |     | Metasys System Client (Any Domain member) SCT (Domain X member) | I/O |   |
|      |                                   |     |   | I/O |   |
| 465  | SMTP                              | TCP | ADS/ADX/OAS/ODS Network Engine                                  | O   | Used for alarms and events  |
| 514  | Syslog                            | UDP | ADS/ADX/OAS/ODS Network Engine SCT                              | O   | Provides capability of sending its configured audit log entries and alarm notifications to the central repository of an external, industry-standard, Syslog server, conforming to Internet published RFC 3164.  |
|      |                                   |     |   | O   |   |
|      |                                   |     |   | O   |   |
| 587  | SMTP                              | TCP | ADS/ADX/OAS/ODS Network Engine                                  | O   | Used for alarms and events  |
|      |                                   |     |   | O   |   |
| 995  | POP3                              | TCP | Computer (Web Browser)  | O   | Receives and holds email for downloading from your Internet server. POP3 is allowed in the Metasys system only for authentication from a SMTP server. The mail server uses port 995 for SSL connections for POP3 access.<br><b>Note:</b> Firewall rules are not necessary to allow access in most cases because this server should be behind the firewall.  |
| 1025 | Remote Procedure                  | TCP | ADS/ADX/OAS/ODS (Domain X member)                               | I/O | Used by IIS on the ADS/ ADX/OAS/ODS/SCT during the process  |



|       |                                    |            |  |                          |   |
|-------|------------------------------------|------------|--|--------------------------|---|
|       | Call (RPC)                         |            | ADX Split<br>Web/Application<br>Server (Domain X<br>member)<br>Metasys System<br>Client (Any Domain<br>member)<br>SCT (Domain X<br>member) | I/O<br>I/O<br>I/O<br>I/O | of authentication during SSO (Windows Integrated Authentication). If SSO is disabled in the Metasys system, this port and protocol are not used by the Metasys system; however, if the ADS/ADX/OAS/ODS/SCT, or Metasys client, or any combination, is a member of an Active Directory service domain, this port and protocol are used for Active Directory service functionality. |
| 1433  | Microsoft SQL Server Database      | TCP        | ADX Metasys ADX Split Database Server (Domain X member)  | I/O                      | Used between the web/ application server and database server computers when the ADX is split across two devices.  |
| 3003  | PhantomJS                          | TCP        | ADS  |                          | Involved in generating PDF files in Metasys UI Reports.   |
| 3389  | Remote Desktop Protocol (RDP)      | TCP        | NAE55/NIE (Windows Embedded OS only)   |                          | Used to log in to the operating system of a device from a remote computer.<br><br>The Remote Desktop Protocol (RDP) Service is usually disabled unless enabled by the NxE Information and Configuration Tool (NCT) operation.   |
| 4096  | NS Protocol                        | UDP        | NAE55 (Windows Embedded OS only)   |                          | Used for N2 tunneling over Ethernet on trunk 1. The N2 technology option provides a serial data port, allowing variable speed drives (VSDs) to link and form a network.   |
| 4097  | NS Protocol                        | UDP        | NAE55 (Windows Embedded OS only)   |                          | Used for N2 tunneling over Ethernet on trunk 2. The N2 technology option provides a serial data port, allowing variable speed drives (VSDs) to link and form a network on the SA Bus.   |
| 9004  | Johnson Controls Licensing Service | TCP        | Software Manager   | I/O                      | For Computer only, it may be closed.  |
| 9910  | Microsoft Discovery Protocol       | TCP<br>UDP | Network Engine<br>SCT<br>NCT and NAE<br>Update Tool  | I<br>I<br>I              | Used by NCT to get diagnostic information from devices on the same network.   |
| 9911  | Metasys Private Message            | UDP        | SCT  | O                        | Used by SCT to broadcast a message to the local network segment when a user selects the device discovery menu item. Any Metasys node that receives this broadcast message will respond on UDP port 9911 with device configuration information to be displayed in the device discovery window.   |
| 10000 | PhantomJS                          | TCP        | ADS  |                          | Involved in generating PDF files in Metasys UI Reports.   |
| 10050 | Johnson Controls Proprietary       | TCP        | NAE Update Tool  | I/O                      | Used during NAE Update Tool operations such as updating an image to a network engine. Not used with SNC and SNE engines prior to Release 10.1.  |
| 11001 | N1 Protocol                        | UDP        | NCM<br>NIE5X   | I/O                      | Provides N1 message transmission (proprietary packet encoded in UDP) for  |

|              |                    |     |                |     |   |
|--------------|--------------------|-----|----------------|-----|---|
|              |                    |     |                |     | devices at Release 9.0 or earlier. If you are connecting to multiple N1 networks, the port is unique for each N1 network. Network Control Modules automatically configure themselves to use Port 11001. Start numbering other networks in the Multinetwork configuration with 11003 and continue sequentially. Do not use a UDP Port Address (UDPPA) of 11002. The value 11002 is used by the Metasys Ethernet Router and should be avoided even if Metasys Ethernet Routers are not in the system. The recommended addressing for five N1s is 11001, 11003, 11004, 11005, 11006. |
| <b>12000</b> | UberDebug Service  | TCP | Metasys System | I/O | Used by Metasys software for debugging and logging.   |
| <b>47808</b> | BACnet/IP Protocol | UDP | NAE/NCE        | I/O | Refer to the BACnet Controller Integration with NAE/NCE Technical Bulletin (LIT-1201531).<br>If you are connecting to multiple BACnet networks, the port is unique for each BACnet network. The default port number is 47808. Choose additional UDP ports that do not conflict with a port that is in use.  |

Table 1.6.1.2: Internal Only Port numbers and protocols

| Port        | Protocol                            | Use | Devices | Description  |
|-------------|-------------------------------------|-----|---------|--|
| <b>3003</b> | PhantomJS                           | TCP | ADS     | Involved in generating PDF files in Metasys UI Reports.              |
| <b>4369</b> | Rabbit MQ                           | TCP | ADS/ADX | Erlang Port Mapping Daemon.  |
| <b>5291</b> | Action Queue                        | TCP | ADS/ADX | Action Queue communication, processing events/audits.                |
| <b>5672</b> | Rabbit MQ/Erlang                    | TCP | ADS/ADX | Listening port for Message Bus, communication between microservices. |
| <b>5960</b> | Device Manager                      | TCP | ADS/ADX | Metasys Device Manager inter-process communication.                  |
| <b>9003</b> | Johnson Controls Product Update     | TCP | ADS/ADX | Port to query for Johnson Controls Product Updates.                  |
| <b>9505</b> | Johnson Controls Rate Limit Website | TCP | ADS/ADX | Website binding to process rate limiting for requests.               |
| <b>9506</b> | Johnson Controls Rewrite Website    | TCP | ADS/ADX | Website binding to route API requests to appropriate micro-services. |

|              |                          |      |         |   |
|--------------|--------------------------|------|---------|---|
| <b>9507</b>  | Johnson Controls Website | TCP  | ADS/ADX | Main internal website binding hosting APIs.             |
| <b>10000</b> | PhantomJS                | TCP  | ADS     | Involved in generating PDF files in Metasys UI Reports. |
| <b>25672</b> | Rabbit MQ/Erlang         | AMQP | ADS/ADX | Inter-node and CLI tool communication.                  |

Table 1.6.1.3: Wireless Port numbers and protocols

| Port         | Protocol                                 | Use | Devices                            | Inbound / Outbound | Description  |
|--------------|--|-----|------------------------------------|--------------------|--|
| <b>80</b>    | HTTP<br>802.11b/802.11g                  | TCP | Computer (Web Browser)             | I                  | Used to synchronize computer clocks over a network between a server and its clients. SNTP is not required for all systems. |
| <b>4050</b>  | Wireless Many-to-One Sensing<br>802.15.4 | UDP | WRS-RTN                            | I/O                | Used for wireless supervisor integration; recommended UDP port number.   |
| <b>47808</b> | Wireless ZigBee<br>802.15.4              | UDP | Wireless Network Coordinator (WNC) | I/O                | Used for wireless supervisor integration; recommended UDP port number.   |

## 1.7.0 Network planning

This section describes network planning including infrastructure protection.

For information on how to plan your Metasys network and implementing virtual networks (VLANs) see document Metasys IP Networks for BACnet/IP Controllers Technical Bulletin (LIT-12012458).

### 1.7.1 Trust boundaries overview

A trust boundary within a system is the boundary in which data is passed between components that do not share an equal level of trust. Products that are not part of the Metasys system or do not provide methods to sufficiently authenticate a component or user may be regarded as having a lower level of trust. Networks may also have different levels of trust. For example, an isolated network with only video cameras and NVRs is usually trusted more than a shared use network such as the corporate IT network or a remote network.

When the trust deviation is beyond the risk tolerance, it is best to control the flow of data between trusted and untrusted network using a switch or router with data flow control capabilities, such as a firewall.

#### 1.7.1.1 Isolated LAN

The Isolated Network architecture is applicable in cases where there is no common IT network (for example, all tenants within a building build out their own private IT networks) or when the BAS network is not allowed to connect to the IT network. An Isolated Metasys BACnet/IP network can also be deployed as a provisional network for new construction prior to the availability of the IT network. The Isolated Metasys BACnet/IP network can then be converted to a Connected Metasys BACnet/IP network once the IT network is available.

### 1.7.1.2 DMZ

The DMZ is a portion of the network located between the Internet and the intranet. It is a buffered area that is usually protected by two or more firewalls.

We do not recommend putting any Metasys equipment in the DMZ.

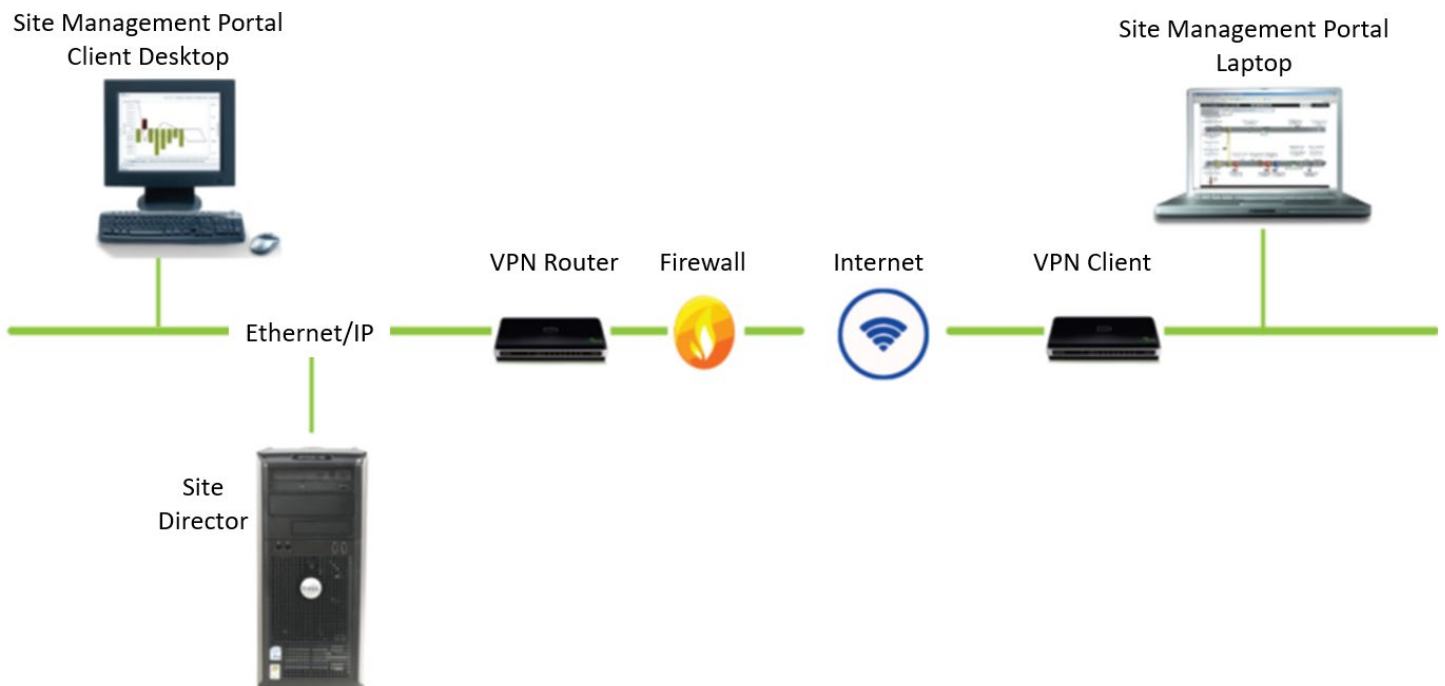
### 1.7.1.3 Firewalls

A firewall is a network security device that monitors, and filters incoming and outgoing network traffic based on an organization's previously established security policies.

### 1.7.1.4 Secure Remote access and VPN

The simplest method of remotely accessing the Metasys system is to use an existing VPN infrastructure. If an existing VPN infrastructure is present on the site already, the risks and security concerns have been established and addressed. Using a VPN, the Metasys system features are the same as if remote users are on the company intranet. The one restriction is that the Metasys system does not support Secure Socket Layer (SSL) VPN.

Figure 1.7.1.4: Metasys system Internet communication by using VPN



### 1.8.0 Hardware and software requirements

Computer minimum hardware configurations are based upon experience and testing for both client and server platforms and are published in the literature for each component of the Metasys system. Follow these requirements.

Computers running Metasys software must perform simultaneous tasks that require both hardware and network resources, and optional or advanced features require a large amount of memory for proper performance. Examples of the optional features of the Metasys system include advanced navigation and support for complex graphics, operation with the maximum number of concurrent users, complex and extended queries with the Metasys Export Utility, support for large network integrations, extensive use of trending, and large numbers of concurrent open applications.

It is important to note that operating systems and computing capabilities change rapidly. A computer that is adequate for today's applications may be inadequate in a year if additional system features and functions become required. Configuration requirements for computers running Metasys software may be upgraded on a regular basis to reflect these changes.

Refer to the Metasys System Configuration Guide (LIT-12011832). See section: Technical specifications and requirements (Pages 74 through 95), for specific computer requirements for all Metasys software products and tools.

**Note:** Certain installations will require additional storage capacity on the system or the ability to offload files to another location. For example: DoD auditing requirements for SQL and IIS. Department of Defense (DoD) auditing requirements for SQL and IIS will require additional storage capacity on the system or the ability to offload files to another location.

## 2 Deployment

The contents within this section address how to initiate secure deployment for new installations, how to harden Metasys and additional steps after commissioning required before turning over Metasys to runtime operations.

### 2.1.0 Deployment overview

Security hardening of Metasys begins prior to deployment with careful planning as outlined in Section 1 of this guide. It is a good practice to review that section prior to deployment to fully understand the security feature set of Metasys, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Resetting factory defaults
- Considerations for commissioning
- Recommended knowledge level

The Metasys Server setup is a comprehensive utility that installs the Metasys Server, third-party components required by the Metasys Server software, and many of the Microsoft® Windows® components required by the Metasys system.

#### 2.1.1 Physical installation considerations

Physical installation considerations of components within your Metasys solution are covered in section 1.3.0 – Intended Environment.

When installing Metasys software, use the instructions provided in the installation guide. Keep in mind that both the physical access and physical installation of the device can impact cybersecurity.

Physical server access enables actions that cannot be authenticated and logged electronically through the capabilities of Metasys. To prevent unauthorized access, be sure to place the device in a room, on a metal panel, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control). When communication wiring goes through areas of lower trust, consider using protective electrical wire conduit.

#### 2.1.2 Getting started

Before installing Metasys, consider the following guidance. Certain products are installed during the installation process while others are optional and not installed. To help you better understand, please review the Metasys Server Installation and Upgrade Guide Release 11.0 document (LIT-12012162).

Operating system patches. You may decide to patch your system before installation of Metasys or after. Please see section 2.4.0 to update Metasys to latest version. Please consult Microsoft for patches available for your server OS.

### 2.1.3 Resetting factory defaults

If a Metasys component was previously used as part of another installation or used in a test environment, the engines should be reset to factory defaults before being put into service in a new deployment. In the case that an engine would need to be sent for repairs, it is advised to first wipe the device clean. To perform the reset, you must use the System Configuration Tool (SCT).

### 2.1.4 Considerations for commission

In some applications the default settings may not be sufficient to fully commission the system. Functions that will not be used during the commissioning process should be disabled.

In the commissioning phase, a less secure configuration may be used before the full infrastructure is available to speed up the deployment process (for example, using wireless). Once the commissioning phase is complete, be sure to remove the temporary infrastructure and harden the system further before turning over to full runtime operations.

### 2.1.5 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in Metasys administration and networking technologies. Completion of the Metasys basic and advanced installation courses is recommended. Please consult the JCI Learning and Development site for course registration.

Helpful training links which require credentials from JCI employees to logon:

- <https://johnsoncontrols.edcast.com/>
- <https://my.jci.com/sites/BESalesOpsLearn/BESalesOpsTech/Pages/welcome.aspx>
- <https://my.jci.com/sites/Training-and-Operations-Support/L&D>

## 2.2.0 Hardening

While Metasys has several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment.

In this section configuration settings labelled as “minimum baseline protection” are provided as general guidance; However, the minimum baseline protection may not be sufficient for the target application. It is important to apply to the correct level of protection as warranted by policies and regulations that may govern the application security settings for a deployment instance of Metasys.

NOTE for US Government installations: U.S. government agencies may have additional hardening requirements. For example, the DoD requires installing SQL and IIS on different drives or partitions. Be sure to reference the applicable Security Technical Implementation Guide (STIG) which list out all the specific software requirements. STIGs can be downloaded from the following public web site:  
<https://public.cyber.mil/stigs/>

### 2.2.1 Hardening checklist

- [Hardening Step 1: Disable TLS 1.0 and 1.1](#)
- [Hardening Step 2: Disable unused Ports](#)
- [Hardening Step 3: User Account Settings](#)
- [Hardening Step 4: Update Metasys to latest version](#)
- [Hardening Step 5: Load TLS certificates](#)
- [Hardening Step 6: Configure Audit log](#)
- [Hardening Step 7: Backup and Restore](#)

### 2.2.2 Disable TLS 1.0 and 1.1

Metasys uses secure HTTP with Transport Layer Security (TLS) 1.2 between the SCT computer, all Metasys servers, and network engines that are upgraded to Metasys Release 9.0 and later. The Windows registry of your computer is used to see which versions of TLS you are using.

#### Hardening Step 1: Disable TLS 1.0 and 1.1.

If your system does not need to use TLS 1.0 and TLS 1.1 and your customer’s IT policy allows the change, we recommend disabling these two versions. Keep TLS version 1.2 and later enabled. For general information on how to implement TLS or SSL, refer to <https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings>.

Note: Ensure that you have all patches of SQL server applied which do not support TLS 1.0 and TLS 1.1.

### 2.2.3 Disable unused Ports

Unused ports should be closed unless they are specifically needed for Metasys or another approved use / application to function. In section 1.6.1 we reviewed the ports and protocols that need to be open based on the features being used.

#### Hardening Step 2: Disable unused ports

Ensure that the ports corresponding to your Metasys system from section 1.6.1 are open. To harden your system, block all ports that are not in use.



### 2.3.0 User management best practices

Following best practices for managing user accounts, account credentials and authorizations (permissions) can greatly improve the security for the system. Some guidance is presented in this section. For additional guidance, NIST standards such as SP 800-63 Digital Identity Guidelines may be consulted.

Do not share accounts. It is best practice to create unique user accounts for each administrator for the Metasys system. The proper configuration of individual user accounts assures that security best practices are followed and that all user actions are audited.

Table 2.3.0

| Feature                             | Description  |
|-------------------------------------|--|
| <b>User account password length</b> | 8-50 characters<br><i>Note: If you're using AD LDAP or ADFS, limitations apply. See specific Metasys or Microsoft documentation.</i>   |
| <b>Inactive Sessions</b>            | 5 minutes timeout (30 is the default)  |
| <b>Password history</b>             | 10 (default)   |
| <b>Maximum Password Age</b>         | 90 days for user level accounts<br>60 days for admin level user accounts   |
| <b>Timesheet</b>                    | The Time Sheet tab allows administrators to place time-of-day restrictions on user login. Users may log in to the system during the selected hours but denied access when they try to log in during unselected hours |
| <b>Temporary user account</b>       | Allows the user to access the system as a temporary user. The user can access the account if it has not expired. When expired, the user is logged out of the system.   |

#### 2.3.1 Metasys User Roles and Permissions

Only Metasys administrators can access the User Management feature. Administrators add existing Active Directory service users to the Metasys system and assign Metasys system privileges using the Security Administrator System.

#### Roles

You can assign a minimum of one of the following roles to the local or Active Directory LDAP user account.

- **User:** Read only access
- **Operator:** Assigned privileges from a list in the User Assigned Dialog Box
- **Maintenance:** Assigned privileges from a list in the User Assigned Dialog Box
- **Administrator:** Access to the full Security Administrator system using the Metasys system online user interface and the SCT

#### Permissions

Add the proper permissions for each user account. Each user can have one type of permission.

- **Standard Access:** The Metasys local system user or Active Directory service user can access all authorized features of the online SMP UI and the SCT. Users can also access the Metasys UI.  
Note: If you have Standard Access and the Advanced Reporting privilege, you can use the Metasys Advanced Reporting System.
- **Tenant Access:** The Metasys local system user or Active Directory service user can access all authorized features of the Metasys UI.

- **API Access:** The Metasys local system user or Active Directory user can access the Metasys Application Programming Interface (API), all authorized features of the Metasys UI and can also access limited features of the SMP UI. Use API access to read and write system data from a custom application or retrieve information from the Metasys system network. See Security Administrator System Technical Bulletin (LIT-1201528) for more details.

**Note:** When you assign a role and permission to a user’s account, apply the principal of least privilege. See section 2.3.6 for more information on applying the least privilege.

Figure 2.3.1.1 – Security Administrator System Screen

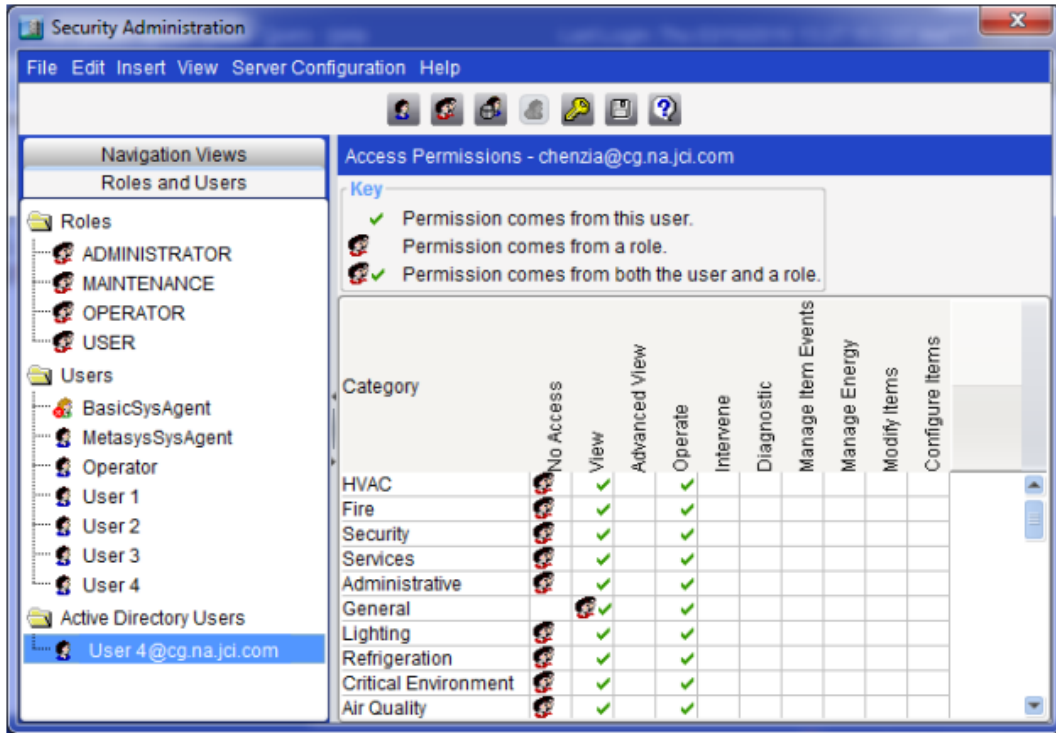


Figure 2.3.1.2 – Metasys UI (MUI) User Management: Users Tab



Figure 2.3.1.3 – Metasys UI (MUI) User Management: Roles Tab



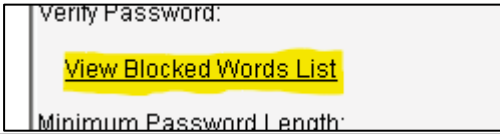
### 2.3.2 Metasys Local User Accounts

Metasys Local Users must use strong or complex passwords, comprised of the criteria shown in table 2.3.1 at a minimum. We recommend suggestions in the right column for further hardening.

#### Hardening Step 3: User Account Settings

To harden your system, update the following settings for user account attributes and policies:

Table 2.3.1 – User Account Passwords criteria

| Attribute                    | Minimum requirement  | Recommended for further hardening  |
|------------------------------|--|--|
| <b>Password total length</b> | 8 characters   | Create passwords of at least 12-15 characters (max 50)                                     |
| <b>Special characters</b>    | 1 character such as<br>-, ., @, #, !, ?, \$, %.<br>All other special characters are invalid, including spaces.   | Include 2 or more non-succession special characters  |
| <b>Upper Case characters</b> | 1 character  | Include 2 or more  |
| <b>Lower Case characters</b> | 1 character  | Include 2 or more  |
| <b>Numbers</b>               | 1 character  | Include 1 or more  |
| <b>Blocked Words List</b>    | Add list of words as suggested from an online Blocked Words List<br> | Add company and product names associated with project (e.g., JCI, Metasys, OpenBlue, etc.) |
| <b>Special rule</b>          | The password cannot contain three consecutive characters from the user account name.   |  |

\* Note: For additional details about the Blocked Words List, view details at his link -

<https://docs.johnsoncontrols.com/bas/r/Metasys/en-US/Security-Administrator-System-Technical-Bulletin/11.0>

Figure 2.3.1.1 SMP UI User Properties Tab

The screenshot shows the 'User Properties' tab for a user named 'Operator'. The interface includes several input fields and checkboxes:

- User Name:** Operator
- Description:** Metasys System Operator
- Password:** [Redacted]
- Verify Password:** [Redacted]
- [View Blocked Words List](#) and [View Password Policy](#) links.
- Minimum Password Length:** 8
- Maximum Password Length:** 50
- Single Access User
- Temporary User
- Expires On:** Monday, October 29, 2018
- User Must Change Password at Next Logon
- User Cannot Change Password
- Account Disabled
- Account Locked Out
- User Can Modify Own Profile
- User Can View the Item Navigation Tree (Default Tree)
- User Can Disable Alarm Pop-Ups
- Access Type:** Standard Access

Figure 2.3.1.2 MUI User Operator Tab

The screenshot shows the 'Operator' user details page in the MUI. It is divided into several sections:

- Operator Profile (Left Sidebar):**
  - Full Name:** Operator
  - Username:** Operator
  - Email:**
  - Role:** OPERATOR
  - Access:** Standard
  - Last Login:** 04/13/2022 9:35 AM
  - Status:** Active
  - Type:** Metasys
- User Details (Main Section):**
  - Full Name:** Operator
  - Description:** Metasys System Operator
  - Username \***: Operator
  - Email:**
  - Phone Number:**
- Account Settings (Main Section):**
  - Actions:**
    - Unlock Account:
    - Force Password Change:
    - Disable Account:
    - User Can View The Item Navigation Tree (Default Tree):
  - New Password:** [Input Field]
  - Confirm New Password:** [Input Field]
  - Password Length:**
    - Minimum Password Length \*: 8
    - Maximum Password Length \*: 50
  - Access Type:** Standard
  - Language:** English (United States)
- System Privileges (Main Section):**
  - Single Access User
  - User Can Modify Own Profile
  - User Cannot Change Password
  - Temporary User
  - Expires On:** 04/13/2022
  - Role \*:** OPERATOR
  - System Privileges:** SELECT...
  - From Role(s):** Discard Acknowledged Events

Buttons for 'CANCEL' and 'SAVE' are located at the bottom right.

### 2.3.3 Metasys LDAP Active Directory User Accounts:

You can log on using your Active Directory username and password if the Active Directory login feature is set up in the Metasys system. Metasys uses LDAP (Lightweight Directory Access Protocol) for directory services authentication. This optional component provides the convenience of Single Sign-On (SSO) access, a capability that permits users to log on to multiple, secured application User Interfaces without re-entering their username and password.

The authentication of the Metasys Active Directory LDAP account happens outside of Metasys. However, when the Domain controller does provide the authentication of the LDAP user account, then the account is granted access to Metasys with the given Metasys permissions set up for that AD LDAP account.

Using the Active Directory LDAP account, you can configure the account's session time out, and the optional timesheet to restrict which days of the weeks and hours of the day the user is allowed to access Metasys. For more information on Active Directory and the Metasys system, refer to the Network and IT Guidance Technical Bulletin (LIT-12011279).

### 2.3.4 No shared accounts

Unique accounts should be used during all phases of operation for Metasys. Installers, technicians, auditors, and other deployment phase users should never share common user accounts to ensure audit trails of their actions.

When user accounts are shared, it no longer becomes possible to determine which specific operator performed actions. We recommend that all users have named accounts, including JCI technicians.

However, there is one Metasys exception to this rule. During a new Metasys deployment, employing multiple installers, you will need to share the **MetasysSysAgent** account. The MetasysSysAgent password should be stored within a password manager so that it can be securely shared with other members of the installation team.

### 2.3.5 Change default passwords

Default passwords should be changed as these published defaults are easily guessed by unauthorized users and automated scripts can use them to gain access.

Note: Since Metasys 6.0, you will be prompted to change your password after first logon.

### 2.3.6 Least privilege

The principal of least privilege means the following:

- Only the minimum necessary rights should be assigned to a user that requests access to Metasys
- Access rights should be in effect for the shortest duration necessary to do their job

Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. The best practice when assigning Metasys access rights is to only give an individual user the necessary role and permissions to their job and nothing more.

### 2.3.7 Separation of duties

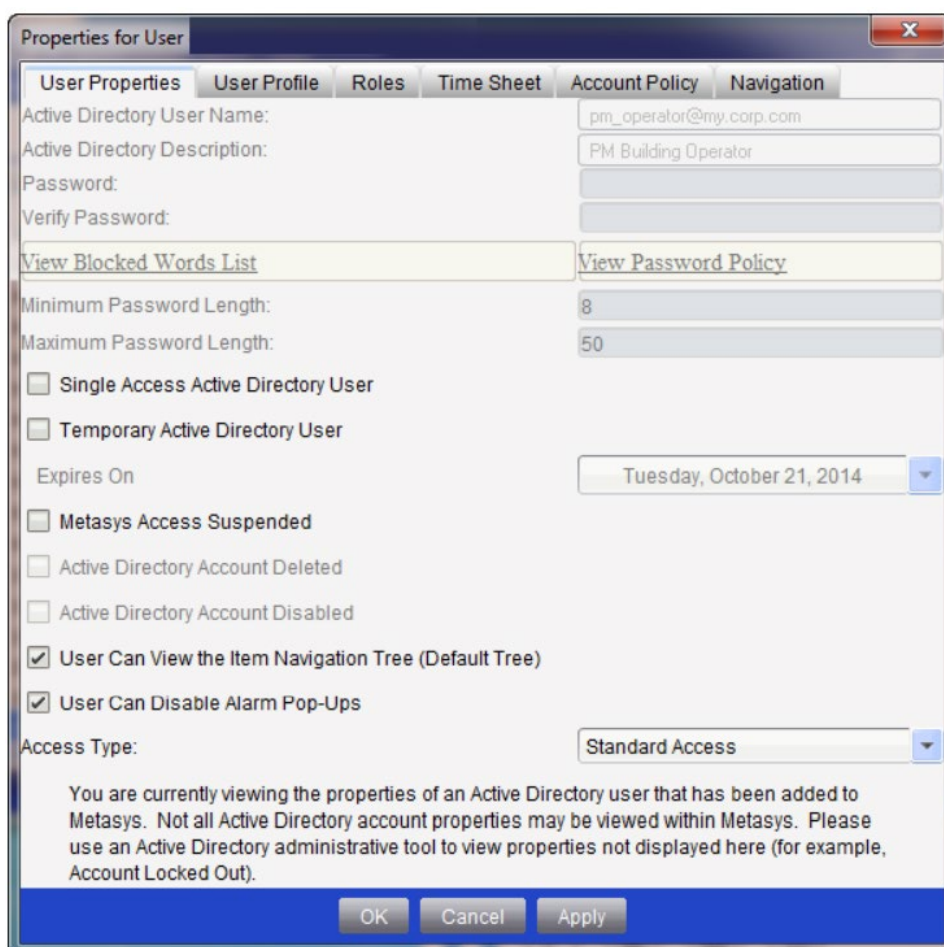
No single user should have full access rights to perform all administrative actions. By separating duties among multiple operators, the amount of power held by a single person is restricted and aids in preventing fraud. Examples of separation of administrative duties - by site, building, sub-system (Fire, HVAC, security),

building owner vs. integrator role, functions (operations vs network management vs. backup). This reduces the risk of insiders successfully committing fraud.

### 2.3.8 Centralized user account management

Identity Management Systems (IDMS) offer enhanced security over the local management of users within Metasys. An IDMS, such as Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) capable IDMS, can provide user account management for multiple devices or systems. By centrally managing user accounts, an administrator can assure consistency throughout the domain the IDMS manages. This assures that when an account is disabled in the domain, access by that user is disabled everywhere in the domain. Furthermore, IDMS provides a centralized location to manage password policies which dictates password formation rules including, length, capitalization, reuse, and expiration. See Security Administrator System Technical Bulletin (LIT-1201528) for more details.

Figure 2.3.8



|  | Required field | Optional field |
|--|----------------|----------------|
| AD Username                            | X              |                |
| Metasys Session Timeout                | X              |                |
| Timesheet                              |                | X              |
| Single access Active Directory user    |                | X              |
| Temporary Active Directory user        |                | X              |
| Metasys access suspended               |                | X              |
| User can view the item navigation tree |                | X              |
| User can disable alarm pop-ups         |                | X              |
| Dormant User account feature           |                | X              |

### 2.3.9 Password policy

Customers often have password policies that all systems must support. Make sure to define the password requirements and the procedures your organization must follow to manage passwords and set a high level of security. Here are some guidelines to follow:

- Passwords are to be treated as sensitive and confidential
- Do not write down passwords where it can be discovered such as on paper, chalkboard, or dry erase boards
- Do not share your passwords with anyone
- Do not use the same passwords for personal use and at work

### 2.3.10 Kiosk Service Accounts

Metasys does not have a user account specifically used for Kiosks. However, the recommendation is to set up a new user account for the Kiosks and allow only view only information with no session timeout.

#### Recommendations

- Name this account a Kiosk account
- You must use a **User** role. Never use an **Administration** role.

### 2.3.11 Radius Accounts

Radius accounts are no longer supported in release 11.0 as they were replaced by FIPS 140-2 support.

### 2.3.12 User management best practices

Following best practices for managing user accounts, their credentials, and authorizations (permissions) can improve the security for the solution.

#### 2.3.12.1 *Centralized user account management*

With Metasys you can use Active Directory LDAP user accounts. A benefit of using Active Directory LDAP accounts is that a customer's IT department can manage Active Directory LDAP Metasys user accounts. While the Active Directory LDAP authentication is done outside of Metasys, each Active Directory LDAP session is given a username in Metasys with the session timeout, dormant user account settings, and timesheets configuration.

Metasys does not store the Active Directory LDAP password. When a user logs on to a computer, Windows caches their Active Directory service credentials and the Metasys system automatically retrieves them during the Windows Integrated Authentication with IIS process on the Metasys server, or SCT.

#### 2.3.12.2 *Strong passwords*

Strong passwords should be used to minimize the risk of password guessing. Automated forms of password guessing such as "dictionary attacks" and "rainbow tables" can run through commonly used passwords and can be successful if strong passwords are not used. You can strengthen a password with length and complexity. The length of a password has the biggest impact on making password guessing difficult.

#### 2.3.12.3 *Password aging*

Password aging is a technique used to reduce to possibility of password exploitation. The **Maximum password age** applies to Metasys Local User accounts. Set the account policy to define a period in days that a user can use a password for before they are prompted to change it. You can set passwords to expire

after a number of days between 1 and 180. To specify that passwords never expire, click **Never Set to Expire**.

**Note:** The Metasys system defaults the Maximum Password Age for an admin user account to 60 days, and the non-admin user accounts to 90 days.

#### 2.3.12.4 Password history

Password histories are used to mitigate against password reuse. Metasys user accounts must abide by the configured password history, with at least 11 previous passwords remembered. For further hardening, refer to the Metasys customer's IT policy on password history. If no such policy exists, leave the password history set to 11 as best practice.

## 2.4.0 Update Metasys to latest version

It is always best practice to harden Metasys by updating to the latest patch version. Patches often contain fixes which strengthen the security of the application.

### Hardening Step 4: Update Metasys to latest version

Patches and updates can include cybersecurity enhancements, as well as fixes to known issues. Review the release notes and prioritize the benefits of the patch or update.

Check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor and update these accordingly.

## 2.5.0 Communication hardening

Communication hardening limits an attacker's ability to gain access to Metasys. Attackers look for weakness in communication protocols, and communications that is left on encrypted and unauthenticated include the risk that the attacker will be successful in their efforts. Employ techniques to harden the communication interfaces and the transmission of data within this section.

### 2.5.1 Least functionality

Least functionality is a security measure designed to limit functions only to those that are required for the target application and communication sessions used at a given time. In configuring components in this manner, the attack surface is reduced and with it the risk of a cybersecurity breach is minimized.

#### 2.5.1.1 Wireless ZFR configuration

The ZFR wireless system extends ZigBee wireless capability to the Metasys BACnet Field Bus. Depending on the model you have, consult the specific configuration guide (such as the ZFR1810 or ZFR1830) to further harden security on this device.

For example, the security features available on the ZFR1830 are:

- Wireless devices can only be added to ZFR mesh network when manually "opened"
- Pre-defined timers automatically close the network to prevent accidental openings
- Standard Zigbee random network keys
- Proprietary key exchange1
- Standard Zigbee AES 128-bit encryption security
- Proprietary ZFR183x messaging structures
- Signed FW Update packages



For more information see the Metasys WRG1830/ZFR183x Pro Series Technical Bulletin (LIT-12013553).

## 2.5.2 Communication certificate support

[Hardening Step 5: Load TLS certificates](#)

General information. HTTPS encrypts communications traffic but does not verify the identity of the remote host without a properly configured digital certificate.

For Metasys Releases 8.1 and higher, a certificate is used between the Metasys application Servers and Engines, and any Metasys client to the Metasys application servers or Metasys engines.

A Self-signed certificate (default certificate) is created at the time of the server installation unless one exists. Group certificates or Certificate Authority (CA) signed certificates are also supported for the Metasys application server and engines.

For more information see the Metasys Release 11.0 Network and IT Guidance Technical Bulletin (LIT-12011279) - Appendix: Certificate management and security.

Note: Wildcard certificates are not supported on Metasys.

Metasys application server specific. Default certificates are self-signed and can only be used for encryption. Privately trusted certificates or CA signed certificates are also supported for the Metasys application server and engines.

See the Metasys Release 11.0 Network and IT Guidance Technical Bulletin (LIT-12011279) - Appendix: Certificate management and security for details how to install the certificates on the Metasys application server.

Metasys engine specific. Use the Certificate Management option in SCT to manage trusted certificates that are stored in network engines. For details, refer to the SNE Commissioning Guide (LIT-1201645) Appendix: Certificate Management.

## 2.5.3 FIPS 140-2 support

FIPS 140-2 was defined by the U.S. government with a purpose of defining how a cryptographic module will protect unclassified, yet sensitive information.

See section 1.2.4 for the standard, definition and how it relates to Metasys. FIPS 140-2 is an optional component. For the server class products ADX/ADS/OAS/NAE8500, one must purchase the FIPS-140-0 product code and license it. The specific product code is M4-FIPS-0.

If you have purchased this add-on option, follow the installation instructions to enable this functionality.

See Metasys Server Installation and Upgrade Instructions (LIT-12012162) for additional details.

## 2.6.0 Configuring security monitoring features

In this section you can find information on configuring security monitoring features.

### 2.6.1 Audit Logs

[Hardening Step 6: Configure Audit log](#)

The Metasys system creates and maintains independent local repositories for events and audits. Metasys System Configuration Guide (LIT-12011832) describes their configuration. Events and audit entries from Metasys can be configured to a customer Syslog server where a customer may elect to look at audits and / or events for logins at odd times, logins from odd locations, or failed login attempts.

MUI Specific. The MUI Cyber Health DB's "User Activity" can give you the number of unsuccessful, successful, and locked user accounts on a daily, weekly, or monthly time period.

SMP UI Specific. The User Logon feature in SMP UI will give you the last date/time of day a user logged into Metasys. In addition, the Metasys Audit Log will show the IP address of the client that you logged in with.

## 2.7.0 Availability hardening

Availability hardening is important to keeping your system up and running.

The three letters in "CIA triad" stand for confidentiality, integrity, and availability. The CIA triad is a common, respected model that forms the basis for the development of security systems and policies. For BAS systems, the main items is the Availability (is the system up and running) then Integrity (are the BAS communications messages unchanged and still intact) and lastly is the confidentiality still intact for the BAS communications.

### 2.7.1 Backup/restore

#### [Hardening Step 7: Backup and Restore](#)

SCT's existing functionality for uploading the archive and security database for an engine and Metasys application server provides the ability to save the Metasys configuration information and even export that data for offsite storage. Engine certificates can also be backed up. Server certificates must be backed up using the Windows Certificate Management features (the Metasys HTTPS certificates). Metasys online server databases (e.g., Historian, Audit, etc.) must be backed up using the Metasys Database Manager (MDM) tool.

More details on the process and tools needed to completely backup and restore a Metasys application server can be found in the Out of Place Upgrade procedure documentation for the Metasys application server.

If a backup program changes attributes in certain Metasys Server files, the Metasys Server may shut down and then restart. To avoid this scenario, we recommend that you avoid backing up the following files and folders, and that you exclude them from any other programs that access these directories in the Metasys Server during times when Metasys needs to remain operational:

- C:\Program Files (x86)\Johnson Controls\MetasysIII
- C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config
- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config
- C:\Program Files (x86)\Johnson Controls\MetasysReports\bin (Metasys Advanced Reporting System only)
- C:\Program Files (x86)\Johnson Controls\MetasysReports\web.config (Metasys Advanced Reporting System only)

See Network and IT Guidance Technical Bulletin (LIT-12011279) for additional guidance.

### 3 Maintain

In section 1.1.2 we stated that many components work together to provide a custom solution. The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels as conditions change for several solutions. This means that some items in the checklist may not be part of your solution and/or within your contract. From the research you gathered in Section 1.x, and the terms within your contract, determine the items in table 3.1.0 that apply to your system and focus on only those items.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors, combined enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of the audit at the time. You may require a higher degree of protection for the environment that Metasys is serving as policies and regulations change over time.

#### 3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site. The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment

See Table 3.1.0 Cybersecurity maintenance checklist on the following page.

Table 3.1.0 – Cybersecurity Maintenance Checklist

| Item | Description   | Immediate | Base on Priority | Daily | Weekly | Monthly | Quarterly | Annual |
|------|---|-----------|------------------|-------|--------|---------|-----------|--------|
| 1    | Backup historical data  |           |                  | ✓     |        |         |           |        |
| 2    | Backup configuration data   | ✓         |                  |       |        |         |           |        |
| 3    | Test backup data  |           |                  |       |        |         | ✓         |        |
| 4    | Disable user accounts of terminated employees                                 | ✓         |                  |       |        |         | ✓         |        |
| 5    | Remove inactive user accounts   |           |                  |       |        | ✓       |           |        |
| 6    | Update user account roles and permissions                                     |           |                  |       |        |         | ✓         |        |
| 7    | Disable unused features, ports, and services                                  |           |                  |       |        |         | ✓         |        |
| 8    | Check for and prioritize advisories or product notices                        |           |                  |       | ✓      |         |           |        |
| 9    | Plan and execute advisory recommendations                                     |           | ✓                |       |        |         |           |        |
| 10   | Check and prioritize software patches and updates                             |           |                  |       | ✓      |         |           |        |
| 11   | Plan and execute software patches and updates                                 |           | ✓                |       |        |         |           |        |
| 12   | Review updates to organizational policies                                     |           |                  |       |        |         |           | ✓      |
| 13   | Review updates to regulations   |           |                  |       |        |         |           | ✓      |
| 14   | Conduct security audits   |           |                  |       |        |         |           | ✓      |
| 15   | Update password policies  |           |                  |       |        |         |           | ✓      |
| 16   | Update as built documentation   | ✓         |                  |       |        |         |           | ✓      |
| 17   | Update standard operating procedures  |           |                  |       |        |         |           | ✓      |
| 18   | Update MUI logon banners  |           |                  |       |        |         |           | ✓      |
| 19   | Renew licensing agreements  |           |                  |       |        |         |           | ✓      |
| 20   | Renew support contracts   |           |                  |       |        |         |           | ✓      |
| 21   | Check for end-of-life announcements and plan for replacements                 |           |                  |       |        |         |           | ✓      |
| 22   | Periodically delete sensitive data in accordance with policies or regulations | ✓         |                  |       |        |         | ✓         |        |
| 23   | Monitor for cyber attacks   | ✓         |                  | ✓     |        |         |           |        |

### 3.1.1 Backup historical data

Historical data, or SQL data for Metasys, can be the most valuable asset within the Metasys system. You can replace or reconstruct everything else. It is recommended that backups are performed frequently, such as daily. With the recent trend of rising ransomware cases, it is also best practice to utilize off-site backups.

| Action                        | Details  | Suggested frequency |
|-------------------------------|--|---------------------|
| <b>Backup historical data</b> | Backup / Restore historical SQL files from Metasys | Daily               |

### 3.1.2 Backup configuration data

If you need to restore or replace a Metasys component it is important to have a backup of its configuration data to minimize the time required to restore its functions.

| Action                           | Details                                    | Suggested frequency |
|----------------------------------|--|---------------------|
| <b>Backup configuration data</b> | Backup / Restore device configuration data | Immediate           |

### 3.1.3 Test backup data

After completing steps 3.1.1 and 3.1.2, and if your job requires this, test your backup data on an “Out of Place Upgrade” Metasys application server. This will provide assurance that the data backups contain the expected data and integrity.

| Action                  | Details   | Suggested frequency |
|-------------------------|---|---------------------|
| <b>Test Backup data</b> | Load data from backup media into a non-production Metasys | Quarterly           |

### 3.1.4 Disable user accounts of terminated employees

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

If you are using Active Directory (AD) services (section 2.3.3), accounts deleted from AD are automatically disabled from Metasys.

| Action               | Details   | Suggested frequency |
|----------------------|---|---------------------|
| <b>Lock accounts</b> | Refer to the Metasys System Administrator System Technical Bulletin Release 11.0 – User properties section. | Immediate           |

Account Disabled

Account Locked Out

Note: In section 1.2.5 we introduced the **Dormant User Account** standalone feature under the Cyber Health Dashboard. When this feature is enabled, it is useful for managing accounts considered dormant or have not been logged into Metasys for a set period, such as 90 days.

### 3.1.5 Remove inactive user accounts

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may not have utilized it for a long period. This suggests that independent of being authorized to use the system, they do not have a need to use the system and you should remove their user account. This is sometimes referred to as a **use it or lose it** policy. This best practice reduces the amount of active user accounts in the system and therefore lowers the potential attack footprint. We suggest this be performed monthly at a minimum. Check with your local policy to determine if this should be performed more frequently.

| Action                          | Details   | Suggested frequency |
|---------------------------------|---|---------------------|
| <b>Remove inactive accounts</b> | Refer to the Metasys System Administrator System Technical Bulletin Release 11.0 – User properties section. | Monthly             |

### 3.1.6 Update user account roles and permissions

While an employee may still be employed by an organization in which the system is owned, managed, serviced, or used by, they may have changed roles or have increased or decrease their need to utilize the system. When adding a role or a permission to a user's account when that user is granted new authorizations due to an organizational role change, be sure to remove Metasys' roles and permissions no longer required or utilized in their new role.

| Action                           | Details   | Suggested frequency |
|----------------------------------|---|---------------------|
| <b>Update user account roles</b> | Refer to the Metasys System Administrator System Technical Bulletin Release 11.0 – User properties section. | Quarterly           |

### 3.1.7 Disable unused features, ports, and services

Reassess the need for optional features, ports, and services that you do not require, and disable them. This practice will lower the attack surface of Metasys resulting in a higher level of protection.

I.e., Feature – Alarm monitor

| Action                          | Details  | Suggested frequency |
|---------------------------------|--|---------------------|
| <b>Disabled unused features</b> | Refer to your product Installation or User manuals. Also refer to sections 1.6.1 and 2.2.3 to disable unused ports | Quarterly           |

### 3.1.8 Check for and prioritize advisories or product notices

Find cybersecurity advisories for Metasys at <https://www.johnsoncontrols.com/cyber-solutions/security-advisories> with a registered user account. User account registration is open to JCI customers and authorized representatives. Some Key points to consider:

- Determine if Metasys is impacted by the conditions outlined in the advisories
- Based on how the Metasys system is deployed, configured, and used, will help determine if the advisory may or may not be of concern
- Referring to as-built documentation of the Metasys system will help with this assessment. A well good set of as-built documentation will identify the number of components impacted and their location.
- While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in your planning to ensure that any issue impacting your system is fully and appropriately addressed in order of priority.

Check for advisories or product notices from third party components such as networking equipment and operating systems by consulting with the respective vendor.

| Action                                     | Details   | Suggested frequency |
|--|---|---------------------|
| <b>Check for and prioritize advisories</b> | Refer to the link above that hosts Metasys advisories and explore each week | Weekly              |

### 3.1.9 Plan and execute advisory recommendations

Follow the plan determined in maintenance step 3.1.8. Consult with all parties who may be impacted by an advisory or downtime and choose the best time for deployment.

| Action   | Details                                   | Suggested frequency |
|--|---|---------------------|
| <b>Plan and execute advisory recommendations</b> | Plan and execute advisory recommendations | Based on priority   |

### 3.1.10 Check and prioritize patches and updates

While a Metasys patch or update may or may not relate to a security advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements also fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk. Be sure also to check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

| Action  | Details   | Suggested frequency |
|---|---|---------------------|
| <b>Check for and prioritize patches and updates</b> | Explore available patches and updates each week | Weekly              |

### 3.1.11 Plan and execute software patches and updates

Follow the plan determined in maintenance step 3.1.10. Consult with all parties who may be impacted by patches, updates or downtime and choose the best time for deployment.

| Action | Details | Suggested frequency |
|--------|---------|---------------------|
|--------|---------|---------------------|

|  |   |                  |
|--|---|------------------|
| <b>Plan and execute software patches and updates</b> | Plan and execute advisory recommendations | Base on priority |
|--|---|------------------|

### 3.1.12 Review updates to organizational policies

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which complied prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies.

| Action                                      | Details   | Suggested frequency |
|---|---|---------------------|
| <b>Review organizational policy updates</b> | Collect most recent security policies for your organization | Annual              |

### 3.1.13 Review updates to regulations

If Metasys is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

| Action                               | Details   | Suggested frequency |
|--------------------------------------|---|---------------------|
| <b>Review updates to regulations</b> | Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration. | Annual              |

### 3.1.14 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, and configuration and threats have likely changed since the last audit. By conducting periodic security audits, you can apply the latest knowledge and reveal gaps in protection previously undetected or created by changes in system use of configuration.

| Action                         | Details   | Suggested frequency |
|--------------------------------|---|---------------------|
| <b>Conduct security audits</b> | Perform the tasks listed on your Security audit checklist | Annual              |

### 3.1.15 Update password policies

Guidance on password policies is evolving. Password policies should be re-assessed periodically to make sure the right policy is in place for the target environment based on current organizational policies, regulations, and guidance from standards organizations such as NIST.

Update password policies as necessary to keep your system secure that are set forth in the Security Administrator System Technical Bulletin (LIT-1201528) local IT policies, and governing bodies.

| Action                          | Details                           | Suggested frequency |
|---------------------------------|-----------------------------------|---------------------|
| <b>Update password policies</b> | See section 2.3.9 Password policy | Annual              |

### 3.1.16 Update as-built documentation

Update as-built documentation if the Metasys system architecture or component configuration significantly changes. Some configuration changes happen without a formal project or plan and if such cases it may be common to negate updating the as-built documentation.

| Action                               | Details  | Suggested frequency           |
|--------------------------------------|--|-------------------------------|
| <b>Update as-built documentation</b> | Update if the Metasys system architecture or component configuration significantly changes | As changes are made or annual |



### 3.1.17 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, they can create, prevent, or close a gap in protection. Therefore, it is important to update standard operating procedures periodically.

| Action                                      | Details  | Suggested frequency |
|---|--|---------------------|
| <b>Update standard operating procedures</b> | Collect standard operating procedures for use of Metasys within the organization | Annual              |

### 3.1.18 Update MUI logon banners

The system use policy details included on logon banners can change over time. Review and update as required.

| Action                      | Details   | Suggested frequency |
|-----------------------------|---|---------------------|
| <b>Update logon banners</b> | Review and modify the MUI logon banner as necessary | Annual              |

### 3.1.19 Renew licensing agreements

Assure that your Metasys software license supports the necessary functions required for your installation.

| Action                            | Details                           | Suggested frequency |
|-----------------------------------|-----------------------------------|---------------------|
| <b>Renew licensing agreements</b> | Collect active licensing details. | Annual              |

### 3.1.20 Renew support contracts

Assure Metasys software support agreement (SSA) and Product Service Agreement (PSA) are up to date.

| Action                         | Details                     | Suggested frequency |
|--------------------------------|-----------------------------|---------------------|
| <b>Renew support contracts</b> | Collect SSA and PSA details | Annual              |

#### Note: **Site subscription services.**

Site subscription services ensure that the subscriber automatically receives every major and minor Metasys release upgrade for either 1 year or 3 years after purchasing the site subscription. The upgrade software on media or disks is no longer sent automatically to the customer when the next release is available. Software is now available for download and licensing through the License Portal. For customer sites that do not have Internet access, an offline method for obtaining a license is available.

For details, refer to Software Manager Help (LIT-12012389).

### 3.1.21 Check for end-of-support / discontinuation information and plan for replacements.

Check with your local Johnson Controls branch for end-of-support announcements a.k.a. discontinuation information and plan for replacements or upgrades, including all Metasys application server operating systems, Metasys SQL supported version databases, network engines, field controllers, I/O level devices and sensors.

| Action   | Details  | Suggested frequency |
|--|--|---------------------|
| <b>Check for discontinuation information and plan for replacements</b> | Collect end-of-support details for your Metasys products through your local office | Annual              |

### 3.1.22 Periodically delete sensitive data in accordance to policies or regulations

Most Metasys components do not collect or store sensitive data. However, in the case that an engine would need to be sent for repairs, it is customary to first wipe the device clean. You should also collect details on policies and regulations that apply to your installation and specific to your local governing bodies.

| Action   | Details   | Suggested frequency |
|--|---|---------------------|
| <b>Periodically delete sensitive data in accordance to policies or regulations</b> | When components are removed from the site, ensure that they are first wiped clean | As required         |

### 3.1.23 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation. Ultimately it is the site owner's responsibility to:

- Review the many tools available to assist with real-time analytics-based detection
- Decide on and fully test the tool in a non-production environment
- Verify that Metasys continues to operate properly after you have installed any security monitoring tools (Johnson Controls can only assist within the guidelines set forth within contractual agreements in force)
- Never install software (or hardware) unless it aligns with the policies of the environment's owner

| Action                           | Details   | Suggested frequency               |
|----------------------------------|---|-----------------------------------|
| <b>Monitor for cyber attacks</b> | Determine which security monitoring tools and services to implement | Run continuously once implemented |

### 3.2.0 Metasys Release schedule

An update to Metasys including new features and security fixes is released approximately every 9 - 18 months depending on the content.

An interim update that will include only updates for the operating system will be released approximately three months after each release unless there is Metasys release within this timeframe.

Each Metasys update undergoes extensive quality assurance testing before being released.

Here are some definitions of terms to help you.

- **Major release.** A major Metasys software release includes significant new products, features, and enhancements. Major releases are indicated by a new major release number followed by a dot zero (x.0). For example, Release 10.0 and Release 11.0 are major releases. Upgrading Release 9.x or 10.x software to Release 11.0 is a major upgrade.
- **Minor release.** A minor Metasys software release provides minor product and feature enhancements. Minor releases are indicated by a new minor release number following the associated major release number. For example, Release 10.1 is a minor release. Therefore, in this example, upgrading Release 10.0 software to Release 10.1 is a minor upgrade.
- **Software license.** A Metasys software package and end-user license agreement is required for each ADS/ADX, ADSLite, ODS, OAS, MVE, NAE85, and LCS85 on a Metasys system site. Each computer or server package on a site must be licensed after a new installation and re-licensed after any major upgrade to the current release. Also, every ADS/ADX that is migrated must be re-licensed after the migration. Many other software applications and tools require licensing. See Licensing information for more details.
- **Metasys for Validated Environments.** Refer to Metasys for Validated Environments, Extended Architecture Catalogue Page (LIT-1900466)
- **Metasys upgrade software.** Upgrade software is current-release Metasys software for upgrading products, such as the ADS/ ADX, OAS, MVE, NAE85, and LCS85, at sites that have a previous major release of the Metasys software already installed (for example, upgrading Release 10.x or earlier software to Release 11.0). Metasys upgrade software packages are identified by a -6 suffix on the product code number.

## Appendix A - Additional Metasys Literature

| Description   | Literature Number | Release |
|---|-------------------|---------|
| Security Administrator System Technical Bulletin                                | LIT-1201528       | 11.x    |
| Metasys System Configuration Guide for Metasys                                  | LIT-12011832      | 11.x    |
| Metasys Help File   | LIT-1201519       | 11.x    |
| Metasys Server Installation and Upgrade Guide                                   | LIT-12012162      | 11.x    |
| Network and IT Guidance Technical Bulletin                                      | LIT-12011279      | 11.x    |
| Metasys IP Networks for BACnet/IP Controllers Technical Bulletin                | LIT-12012458      | 11.x    |
| Metasys MUI   | LIT-12011953      | 11.x    |
| Software Manager Help   | LIT-12012389      | 11.x    |
| System Configuration Tool Catalog Page  | LIT-1900198       | 14.x    |
| BACnet Controller Integration with NAE/NCE Technical Bulletin                   | LIT-1201531       | 11.x    |
| Metasys Performance Verification Tool (PVT) User Guide                          | LIT-12012406      | 3.x     |
| Metasys System Product Bulletin   | LIT-1201526       | 11.x    |
| Metasys WRG1830/ZFR183x Pro Series Wireless Field Bus System Technical Bulletin | LIT-12013553      | 1.x     |

[Product Documentation | Johnson Controls](#)

## Appendix B - Acronyms

| Acronym      | Description                                       |
|--------------|---|
| <b>AD</b>    | Active Directory                                  |
| <b>ADFS</b>  | Active Directory Federation Services              |
| <b>ADS</b>   | Application Data Server                           |
| <b>ADX</b>   | Extended Application Data Server                  |
| <b>AHU</b>   | Air Handler Unit                                  |
| <b>API</b>   | Application Programming Interface                 |
| <b>BAC</b>   | Building Automation Control/Controller            |
| <b>BFT</b>   | Background File Transfer                          |
| <b>CA</b>    | Certificate Authority                             |
| <b>CCT</b>   | Controller Configuration Tool                     |
| <b>CGE</b>   | General Purpose Application Controller (ethernet) |
| <b>CGM</b>   | General Purpose Application Controller (MS/TP)    |
| <b>CVM</b>   | VAV Box Controller                                |
| <b>DoD</b>   | Department of Defense                             |
| <b>EMC</b>   | Electromagnetic Compatibility                     |
| <b>EMI</b>   | Electromagnetic Interference                      |
| <b>FAC</b>   | Field Application Controller                      |
| <b>FAA</b>   | Federal Aviation Administration                   |
| <b>FEC</b>   | Field Equipment Controller                        |
| <b>FIPS</b>  | Federal Information Processing Standard           |
| <b>GGT</b>   | Graphic Generating Tool                           |
| <b>GSA</b>   | General Services Administration                   |
| <b>HTTP</b>  | Hypertext Transfer Protocol                       |
| <b>HTTPS</b> | Hypertext Transfer Protocol Secure                |
| <b>IDMS</b>  | Identity Management System                        |
| <b>IOM</b>   | Input/Output Modules                              |
| <b>IP</b>    | Internet Protocol                                 |
| <b>LDAP</b>  | Lightweight Directory Access Protocol             |
| <b>MDM</b>   | Metasys Database Manager tool                     |
| <b>MFA</b>   | Multi-Factor Authentication                       |
| <b>MRP</b>   | Media Redundancy Protocol                         |
| <b>MUI</b>   | Metasys User Interface                            |
| <b>MVE</b>   | Metasys for Validated Environments                |
| <b>NAE</b>   | Network Automation Engine                         |
| <b>NCE</b>   | Network Control Engine                            |
| <b>NCT</b>   | NAE information and Configuration Tool            |
| <b>NIE</b>   | Network Integration engine                        |
| <b>NMS</b>   | Network Management System                         |
| <b>OAS</b>   | Open Application Server                           |
| <b>ODS</b>   | Open Data Server                                  |
| <b>PSA</b>   | Product Service Agreement                         |
| <b>RDP</b>   | Remote Desktop Protocol                           |
| <b>RNI</b>   | Remote Network Interface                          |
| <b>RPC</b>   | Remote Procedure Call                             |
| <b>SA</b>    | Sensor Actuator                                   |
| <b>SCT</b>   | Software Configuration Tool                       |
| <b>SMP</b>   | Site Management Portal                            |
| <b>SNC</b>   | Series Network Control Engine                     |

|             |                                      |
|-------------|--------------------------------------|
| <b>SNE</b>  | Series Network Engine                |
| <b>SNMP</b> | Simple Network Management Protocol   |
| <b>SSA</b>  | Software Service Agreement           |
| <b>SSL</b>  | Secure Socket Layer                  |
| <b>SSO</b>  | Single Sign On                       |
| <b>TCP</b>  | Transmission Control Protocol        |
| <b>TEC</b>  | Terminal Equipment Controller        |
| <b>TLS</b>  | Transport Layer Security             |
| <b>UDP</b>  | User Datagram Protocol               |
| <b>UI</b>   | User Interface                       |
| <b>UNT</b>  | Unitary Controller                   |
| <b>VAV</b>  | Variable Air Volume                  |
| <b>VLAN</b> | Virtual Local Area Network           |
| <b>VMA</b>  | Variable air volume Modular Assembly |
| <b>VSD</b>  | Variable Speed Drives                |
| <b>WNC</b>  | Wireless Network Coordinator         |
| <b>XPM</b>  | Expansion Modules                    |

## Appendix C – FAQs

The following examples are the types of hardening/security settings and questions IT departments ask about or put in place.

Q1. Disabling HTTP OPTIONS and Trace commands in IIS?

A1. This is already done in MUI. This cannot be set globally in IIS.

Q2. Can X-Frame headers be set to Deny globally in IIS?

A2. This is already done in MUI. X-Frame cannot be set globally in IIS because in MUI, the PPA/Fault widget runs under its own web application/distinct Angular in an Iframe, so option it needs to use is:

Q3. Can strict transport security (HSTS) be enabled globally in IIS?

A3. HSTS – Metasys SOAP and REST APIs return this response header. This cannot be globally set in IIS because IIS doesn't support multiple layers adding the same header.

Q4. Can the SA Account be completely disabled in SQL?

A4. This can be done, nothing in Metasys uses the SQL sa account.

(Note: they will still have a sysadmin account just wish to disable an account using that name as it is well known)

Q5. How is Kerberos used in AD LDAP?

A5. From the Metasys process we use the .NET component System.DirectoryServices to facilitate the LDAP query to Active Directory. Customers can enable/disable LDAP protocols independent of Metasys.

Q6. Can the public role in SQL be locked down?

A6. Yes, Metasys does not use SQL public role for any purpose.

Q7. Can MSEA\_AppPool in IIS run under an application pool identity instead of Local System

A7. Not at Metasys Release 11.0.

Q8. Can the site specify/manage the list of local administrators on the machine via group policy or will this conflict/create problems for Metasys?

A8. Metasys does not use local administrators group in any way.

Q9. Does Metasys support API Keys for email authentication?

A9. Metasys does not support API Keys at this time for email authentication.

Q10. Does Metasys support wildcard SSL certificates?

A10. Wildcard SSL certificates are not supported.

Q11. Does Metasys use Group Managed Service Accounts for MSSQLSERVER or SSO?

A11. Metasys does not use local groups, domain groups, or SQL Server groups for any purpose.